TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Minna Salmi

Pseudoalkuluvuista ja alkulukutestauksesta

Luonnontieteiden tiedekunta
Matematiikka
Kesäkuu 2017

Tampereen yliopisto
Luonnontieteiden tiedekunta
SALMI, MINNA: Pseudoalkuluvuista ja alkulukutestauksesta
Pro gradu -tutkielma, 49 s.
Matematiikka
Kesäkuu 2017

Tiivistelmä

Tämän tutkielman aiheena on pseudoalkuluvut ja alkulukutestaus. Aluksi käydään läpi joitakin yksinkertaisia tuloksia kongruensseihin liittyen sekä tarvittavia määritelmiä. Alussa osoitetaan myös joitakin isompia apulauseita, jotka ovat hyvin oleellisia tutkielmassa. Tärkeimmät läpikäytävät apulauseet ovat Fermat'n pieni lause, jota käytetään läpi tutkielman, kiinalainen jäännöslause sekä resiprookkilause.

Ensimmäisenä isona kokonaisuutena käydään läpi pseudoalkuluvut. Ensin pseudoalkuluvut määritellään, jonka jälkeen osoitetaan muutamia lauseita pseudoalkulukuihin liittyen ja lauseita havainnollistetaan esimerkein. Seuraavaksi käsitellään erilaisia pseudoalkulukutapauksia tärkeimpinä mainittakoon vahvat pseudoalkuluvut sekä Eulerin pseudoalkuluvut.

Toinen kokonaisuus tutkielmassa on alkulukutestaus. Aluksi kerrataan Fermat'n pieni lause, koska sitä käytetään lähes kaikissa käsiteltävissä alkulukutesteissä. Suurin osa läpikäytävistä testeistä on deterministisiä eli antavat varman vastauksen kysymykseen luvun jaottomuudesta. Käsiteltävät deterministiset alkulukutestit ovat Pepinin, Lucas's ja Lehmerin, Pocklingtonin sekä Millerin ja Rabinin alkulukutestit. Viimeisenä esitellään Solovayn ja Strassenin probabilistinen alkulukutesti. Solovayn ja Strassenin testi antaa todennäköisen vastauksen kysymykseen, onko luku alkuluku.

Sisältö

1 Johdanto

Alkulukujen tutkiminen on kiinnostanut matemaatikkoja läpi aikojen. Aluksi monilla oli tavoitteena löytää jokin yleispätevä kaava, jonka avulla saataisiin kaikki mahdolliset alkuluvut. Tällaista kaavaa ei kuitenkaan tähän päivään mennessä ole löytynyt, mutta on kuitenkin löydetty tiettyjä ominaisuuksia, jotka vain alkuluvuilla on. Esimerkiksi Fermat väitti kehittäneensä kaavan, jonka tuloksena saataisiin pelkkiä alkulukuja. Fermat'n kaava ei pitänyt paikkaansa, mutta sen pohjalta on kehitetty testi, jolla voidaan osoittaa, onko luku alkuluku.

Koska matemaatikot luulivat aina välillä kehittäneensä kaavoja alkuluvuille, mutta aina kaavat todistettiin vääriksi, kehitettiin käsitä pseudoalkuluku. Pseudoalkuluvulla tarkoitetaan yhdistettyjä lukuja, joilla on ominaisuuksia, joiden joskus luultiin kuuluvan vain alkuluvuille. Pseudoalkuluvuilla on tärkeä tehtävä julkisen avaimen salauksissa, joissa käytetään hyväksi vaikeutta jakaa isoja lukuja tekijöihin.

Vaikka yleispätevää kaavaa alkuluvuille ei ole löytynyt, on kuitenkin olemassa monia ominaisuuksia, joita on vain alkuluvuilla. Alkulukutestaus ei anna luvun tekijähajoitelmaa, mutta kertoo kuitenkin testistä riippuen joko että luku on alkuluku tai että luku on yhdistetty. Alkulukutestejä on kahdenlaisia. Deterministiset testit kertovat varmasti onko käsiteltävä luku alkuluku. Probabilistiset testit antavat todennäköisyyden, jolla luku on alkuluku. Olisi helppoa ajatella, että aina kannattaisi käyttää deterministiä testejä, mutta todellisuus on kuitenkin toinen. Deterministiset testit ovat usein aikaavieviä ja sitä kautta kalliita käyttää. Probabilistiset testit ovat usein nopeampia ja antavat yleensä tarpeeksi hyvän todennäköisyyden, jotta niitä kannattaa käyttää.

Tässä tutkielmassa käydään ensin läpi tarvittavia apulauseita, jotka auttavat ymmärtämään tutkielmasssa esitettyjä lauseita. Ensimmäinen isompi kokonaisuus, joka käydään läpi, on pseudoalkuluvut. Aluksi pseudoalkuluvut määritellään, jonka jälkeen esitetään tärkeitä lauseita ja esimerkkejä niistä. Toinen kokonaisuus on alkulukutestaus. Kokonaisuudessa käydään läpi erilaisia alkulukutestejä ja niitä avataan esimerkkien avulla. Alkulukutesteistä esitellään sekä deterministisiä että probabilistisia testejä.

Tässä tutkielmassa odotetaan lukijalta jonkin verran ymmärrystä lukuteoriasta ja erityisemmin kongruensseista. Päälähdeteoksena on käytetty Rosenin kirjaa Elementary Number Theory and Its Applications, 6th ed. Lisälähteinä on käytetty useita lukuteoriaan tai kryptografiaan liittyviä kirjoja, ja lopussa lähteenä on käytetty Kevin Conradin esseetä Solovayn Strassenin alkulukutestiä käsiteltävässä luvussa.

2 Aputuloksia

Tässä luvussa käydään läpi joitakin tarvittavia määritelmiä ja lauseita. Ensimmäisen aliluvun tarkoitus on palauttaa lukijalle mieleen muutamia kongruensseihin sekä yleisemmin myös jaollisuuteen liittyviä ominaisuuksia. Toisessa aliluvussa käydään läpi Fermat'n pieni lause, jota käytetään useasti myös seuraavissa luvuissa. Kolmannessa kohdassa käydään läpi tarvittavia määritelmiä esimerkiksi kertaluvusta, Jacobin symbolista sekä matriiseista. Viimeinen aliluku koostuu isommista tärkeistä lauseista, joita käytetään seuraavissa luvuissa.

2.1 Joitakin tarvittavia kongruensseja

Määritelmä 2.1. Oletetaan, että $a \in \mathbb{Z}$ ja $n \in \mathbb{N}$ siten, että $\text{syt}(a, n) = 1$. Kokonaisluvun a käänteisluku modulo n on kokonaisluku x, mikäli $ax \equiv 1 \pmod{n}$. Merkitään luvun a käänteislukua symbolilla $\overline{a}$.

Lause 2.1. *Olkoon p alkuluku. Positiivinen kokonaisluku a on itsensä käänteisluku modulo p, jos ja vain jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$.*

Todistus. (Ks. [8, s. 160].) Jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$, niin $a^2 \equiv 1 \pmod{p}$, joten a on itsensä käänteisluku modulo p.

Toisaalta, jos a on itsensä käänteisluku modulo p, niin $a^2 = a \cdot a \equiv 1 \pmod{p}$. Tällöin $p \mid (a^2 - 1)$. Koska $a^2 - 1 = (a - 1)(a + 1)$, joko $p \mid (a - 1)$ tai $p \mid (a + 1)$. Nyt siis pätee $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$. □

Lause 2.2 (Wilsonin lause)**.** *Jos p on alkuluku, niin $(p - 1)! \equiv -1 \pmod{p}$.*

Todistus. (Vrt. [8, s. 218].) Kun $p = 2$, saadaan $(p - 1)! \equiv 1 \equiv -1 \pmod{2}$. Siis Wilsonin teoreema pätee, kun $p = 2$. Oletetaan nyt, että alkuluku p on suurempi kuin 2. Määritelmän 2.1 perusteella jokaiselle kokonaisluvulle a, kun $1 \leq a \leq p - 1$, on olemassa käänteisluku $\overline{a}$ siten, että $a\overline{a} \equiv 1 \pmod{p}$. Lauseen 2.1 nojalla $a = \overline{a}$, jos ja vain jos $a = 1$ tai $a = p - 1$, eli kaikilla $a \in \{2, 3, \ldots, p - 2\}$ pätee, että $a \neq \bar{a}$. Koska jokaiselle luvulle a on olemassa kokonaisluku $\bar{a} \in \{2, 3, \ldots, p - 2\}$ siten, että $a\bar{a} \equiv 1 \pmod{p}$, kokonaisluvut luvusta 2 lukuun $p - 2$ voidaan jakaa $(p - 3)/2$ kokonaislukupariin siten, että jokaisen parin tulo on kongruentti luvun 1 kanssa modulo p. Siis

$$2 \cdot 3 \cdot \cdots \cdot (p - 3) \cdot (p - 2) \equiv 1 \pmod{p}.$$

Nyt kongruenssin molemmat puolet kerrotaan luvuilla 1 ja $p - 1$, ja näin saadaan

$$(p - 1)! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p - 3)(p - 2)(p - 1) \equiv 1 \cdot (p - 1) \equiv -1 \pmod{p}.$$

□

Lause 2.3 (Käänteinen Wilsonin lause)**.** *Jos n on positiivinen kokonaisluku siten, että $(n - 1)! \equiv -1 \pmod{n}$, niin n on alkuluku.*

Todistus. (Vrt. [7, s. 199].) Tehdään aluksi vastaoletus, että n on yhdistetty luku ja $(n-1)! \equiv -1 \pmod{n}$. Koska n on yhdistetty luku, niin se voidaan kirjoittaa muodossa $n = ab$, missä $1 < a < n$ ja $1 < b < n$. Koska $a < n$, niin tiedetään, että $a \mid (n-1)!$. Näin on, koska a on yksi niistä luvuista, jotka kerrotaan, jotta saadaan $(n-1)!$. Nyt koska $(n-1)! \equiv -1 \pmod{n}$ ja $a \mid n$, niin $(n-1)! \equiv -1 \pmod{a}$. Siis $a \mid (n-1)! + 1$ ja $a \mid (n-1)!$. Tästä seuraa, että $a \mid \big((n-1)! + 1 - (n-1)!\big) = 1$, mikä on ristiriita. □

Lause 2.4. *Jos a, b, c ja m ovat kokonaislukuja siten, että $m > 0$, $d = \text{syt}(c, m)$ ja $ac \equiv bc \pmod{m}$, niin $a \equiv b \pmod{\frac{m}{d}}$.*

Todistus. (Ks. [8, s. 149].) Jos $ac \equiv bc \pmod{m}$, niin tiedetään, että $m \mid (ac - bc) = c(a-b)$. Siis on olemassa kokonaisluku k siten, että $c(a-b) = km$. Jakamalla molemmat puolet luvulla d saadaan

$$\frac{c}{d}(a-b) = k\frac{m}{d}.$$

Koska

$$\text{syt}(\frac{m}{d}, \frac{c}{d}) = 1,$$

niin tästä seuraa, että $\frac{m}{d} \mid (a-b)$. Siis $a \equiv b \pmod{\frac{m}{d}}$. □

Seuraus 2.1. *Jos a, b, c ja m ovat kokonaislukuja niin, että $m > 0$, $\text{syt}(c, m) = 1$ ja $ac \equiv bc \pmod{m}$, niin $a \equiv b \pmod{m}$.*

Todistus. Kyseinen seuraus on lauseen 2.4 erityistapaus. □

Lause 2.5. *(Ks. [8, s. 151].) Olkoon $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, missä $a, b, m_1, m_2, \ldots, m_k$ ovat kokonaislukuja ja luvut $m_1, m_2, \ldots, m_k$ ovat positiivisia. Silloin pätee*

$$a \equiv b \pmod{\text{pyj}(m_1, m_2, \ldots, m_k)},$$

missä $\text{pyj}(m_1, m_2, \ldots, m_k)$ on lukujen $m_1, m_2, \ldots, m_k$ pienin yhteinen jaettava.

Todistus. Koska $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, tiedetään, että $m_1 \mid (a-b)$, $m_2 \mid (a-b)$, $\ldots$, $m_k \mid (a-b)$. Nyt

$$\text{pyj}(m_1, m_2, \ldots, m_k) \mid (a-b).$$

Näin ollen

$$a \equiv b \pmod{\text{pyj}(m_1, m_2, \ldots, m_k)}.$$

□

Lause 2.6. *Jos $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$,...,$a \equiv b \pmod{m_k}$, missä a ja b ovat kokonaislukuja ja luvut $m_1, m_2, \ldots, m_k$ ovat pareittain keskenään jaottomia, niin*

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

Todistus. (Ks. [8, s. 151].) □

Lause 2.7. *Olkoot a ja b kokonaislukuja siten, että* $\text{syt}(a, b) = d$. *Yhtälöllä $ax + by = c$ ei ole kokonaislukuratkaisuja, jos $d \nmid c$. Jos taas $d \mid c$, on kokonaislukuratkaisuja olemassa ääretön määrä.*

Erityisesti jos $x = x_0$, $y = y_0$ on yhtälön ratkaisu, niin silloin kaikki ratkaisut ovat muotoa

$$x = x_0 + (b/d)n, \qquad y = y_0 - (a/d)n,$$

missä n on kokonaisluku.

Todistus. (Ks. [8, s. 138-139].) □

Lause 2.8. *Olkoot a, b ja m kokonaislukuja siten, että $m > 0$ ja* $\text{syt}(a, m) = d$. *Jos $d \nmid b$, kongruenssilla $ax \equiv b \pmod{m}$ ei ole ratkaisuja. Jos $d \mid b$, lausekkeella $ax \equiv b \pmod{m}$ on täsmälleen d kappaletta epäkongruentteja ratkaisuja modulo m.*

Todistus. (Ks. [8, s. 158].) Lineaarinen kongruenssi $ax \equiv b \pmod{m}$ on ekvivalentti Diofantoksen yhtälön $ax - my = b$ kanssa. Kokonaisluku x on kongruenssin $ax \equiv b \pmod{m}$ ratkaisu, jos ja vain jos on olemassa kokonaisluku y siten, että $ax - my = b$. Lauseen 2.7 perusteella tiedetään, että jos $d \nmid b$, ei ole olemassa yhtään ratkaisuja ja toisaalta, jos $d \mid b$, yhtälöllä $ax - my = b$ on olemassa ääretön määrä ratkaisuja, jotka ovat muotoa

$$x = x_0 + (m/d)t, \qquad y = y_0 + (a/d)t,$$

missä $x = x_0$, $y = y_0$ on eräs yhtälön ratkaisu. Luvun $x = x_0 + (m/d)t$ ylläannetut arvot ovat lineaarisen kongruenssin ratkaisuja ja näitä lukuja x on olemassa ääretön määrä.

Jotta voidaan määrittää kuinka monta epäkongruenttia ratkaisua on olemassa, täytyy löytää se ehto, joka kertoo milloin kaksi ratkaisua $x_1 = x_0 + (m/d)t_1$ ja $x_2 = x_0 + (m/d)t_2$ ovat kongruentteja modulo m. Jos nämä ratkaisut ovat kongruentteja, niin pätee

$$x_0 + (m/d)t_1 \equiv x_0 + (m/d)t_2 \pmod{m}.$$

Vähentämällä x_0 pois molemmilta puolilta saadaan

$$(m/d)t_1 \equiv (m/d)t_2 \pmod{m}.$$

Nyt $\text{syt}(m, m/d) = m/d$, koska $(m/d) \mid m$, joten

$$t_1 \equiv t_2 \pmod{d}.$$

Tästä nähdään, että täydellinen epäkongruenttien ratkaisujen joukko koostuu ratkaisuista, jotka ovat muotoa $x = x_0 + (m/d)t$, missä luku t käy läpi kaikki jakojäännökset modulo d. Yksi näistä joukoista saadaan, kun $x = x_0 + (m/d)t$, missä $t = 0, 1, 2, \ldots, d - 1$. □

2.2 Fermat'n pieni lause

Lause 2.9 (Fermat'n pieni lause)**.** *Jos p on alkuluku ja a on positiivinen kokonaisluku siten, että $p \nmid a$, silloin*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Todistus. (Vrt. [8, s. 219].) Huomataan ensimmäiseksi, että mikään kokonaisluvuista $a, 2a, \ldots, (p-1)a$ ei ole jaollinen luvulla p. Nimittäin jos $p \mid ja$ olisi voimassa, niin $p \mid j$, koska $p \nmid a$. Nyt $p \mid j$ ei voi pitää paikkaansa, koska $1 \leq j \leq p-1$. Edelleen mitkään kaksi erisuurta kokonaislukua joukosta $a, 2a, \ldots, (p-1)a$ eivät ole kongruentteja modulo p. Oletetaan, että

$$ja \equiv ka \pmod{p},$$

missä $1 \leq j < k \leq p-1$. Nyt seurauksen 2.1 mukaan, koska $\text{syt}(a, p) = 1$, saadaan $j \equiv k \pmod{p}$. Tämä ei voi pitää paikkaansa, koska j ja k ovat lukua $p-1$ pienempiä erisuuria positiivisia kokonaislukuja.

Koska kokonaisluvut $a, 2a, \ldots, (p-1)a$ ovat joukko, joka koostuu $p-1$ kappaleesta kokonaislukuja, jotka kaikki ovat epäkongruentteja luvun 0 kanssa ja mitkään kaksi eivät ole kongruentteja modulo p, tiedetään, että pienimmät positiiviset jäännökset ovat $1, 2, \ldots, p-1$. Tästä seuraa, että kokonaislukujen $a, 2a, \ldots, (p-1)a$ tulo on kongruentti lukujen $1, 2, \ldots, p-1$ tulon kanssa modulo p. Siis

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Eli siis

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Koska $\text{syt}((p-1)!, p) = 1$, niin seurauksen 2.1 perusteella luku $(p-1)!$ voidaan jakaa pois molemmilta puolilta, jolloin saadaan

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Lause 2.10. *Jos p on alkuluku ja a on positiivinen kokonaisluku, niin*

$$a^p \equiv a \ (mod\ p).$$

Todistus. (Ks. [8, s. 220].) Jos $p \nmid a$, Fermat'n pienen lauseen perusteella tiedetään, että $a^{p-1} \equiv 1 \pmod{p}$. Kertomalla kongruenssin molemmat puolet luvulla a, saadaan $a^p \equiv a \pmod{p}$.

Jos $p \mid a$, silloin myös $p \mid a^p$, joten $a^p \equiv a \equiv 0 \pmod{p}$. Täten $a^p \equiv a \pmod{p}$. □

Lause 2.11. *Jos a ja m ovat keskenään jaottomia alkulukuja siten, että $m > 0$ ja b on kokonaisluku, silloin lineaarisella kongruenssilla $ax \equiv b \pmod{m}$ on yksikäsitteinen ratkaisu modulo m.*

Todistus. (Ks. [8, s. 158].) Koska $\text{syt}(a, m) = 1$, tiedetään, että $\text{syt}(a, m) \mid b$. Lauseesta 2.8 seuraa, että kongruenssilla $ax \equiv b \pmod{m}$ on täsmälleen $\text{syt}(a, m) = 1$ epäkongruenttia ratkaisua modulo m. □

2.3 Tarvittavia määritelmiä kertaluvusta matriiseihin

Määritelmä 2.2. Olkoon n positiivinen kokonaisluku. Eulerin ϕ-funktion arvon $\phi(n)$ määritellään tarkoittavan niiden positiivisten kokonaislukujen m määrää, jotka ovat pienempiä kuin n siten, että n ja m ovat keskenään jaottomia, eli

$$\phi(n) =\mid \{m \mid 0 \leq m < n-1, \text{syt}(m,n) = 1\} \mid .$$

Lause 2.12 (Eulerin lause)**.** *Jos m on positiivinen kokonaisluku ja a on kokonaisluku niin, että* $\text{syt}(a,m) = 1$*, silloin* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Todistus. (Ks. [8, s.236-237].) □

Määritelmä 2.3. Olkoot a ja n keskenään jaottomia alkulukuja siten, että $a \neq 0$ ja n on positiivinen. Silloin pienintä sellaista positiivista kokonaislukua x, että $a^x \equiv 1 \pmod{n}$, kutsutaan luvun a kertaluvuksi modulo n ja kertalukua merkitään symbolilla $\text{ord}_n a$.

Lause 2.13. *Jos luvut a ja n ovat keskenään jaottomia alkulukuja siten, että $a \neq 0$ ja $n > 0$, positiivinen kokonaisluku x on kongruenssin $a^x \equiv 1 \pmod{n}$ ratkaisu, jos ja vain jos* $\text{ord}_n\, a \mid x$.

Todistus. (Ks. [8, s. 348].) Jos $\text{ord}_n a \mid x$, niin $x = k \cdot \text{ord}_n a$, missä k on positiivinen kokonaisluku. Siis

$$a^x = a^{k \cdot \text{ord}_n a} = (a^{\text{ord}_n a})^k \equiv 1 \pmod{n}.$$

Päinvastoin, jos $a^x \equiv 1 \pmod{n}$, saadaan

$$x = q \cdot \text{ord}_n a + r,$$

missä $0 \leq r < \text{ord}_n a$. Ylläolevasta yhtälöstä saadaan

$$a^x = a^{q \cdot \text{ord}_n a + r} = (a^{\text{ord}_n a})^q a^r \equiv a^r \pmod{n}.$$

Koska $a^x \equiv 1 \pmod{n}$, tiedetään, että $a^r \equiv 1 \pmod{n}$. Epäyhtälöstä $0 \leq r < \text{ord}_n a$ seuraa, että $r = 0$, koska määritelmän mukaan $y = \text{ord}_n a$ on pienin positiivinen kokonaisluku siten, että $a^y \equiv 1 \pmod{n}$. Koska $r = 0$, saadaan $x = q \cdot \text{ord}_n a$. Siis $\text{ord}_n a \mid x$. □

Määritelmä 2.4. Jos luvut r ja n ovat keskenään jaottomia lukuja siten, että $n > 0$, ja jos $\text{ord}_n r = \phi(n)$, niin lukua r kutsutaan primitiiviseksi juureksi modulo n tai luvun n primitiiviseksi juureksi, ja tällöin voidaan sanoa, että luvulla n on primitiivinen juuri.

Määritelmä 2.5. Jos m on positiivinen kokonaisluku, sanotaan, että kokonaisluku a on luvun m neliönjäännös, jos $\text{syt}(a,m) = 1$ ja kongruenssilla $x^2 \equiv a \pmod{m}$ on ratkaisu. Jos kongruenssilla $x^2 \equiv a \pmod{m}$ ei ole ratkaisua, sanotaan, että luku a on luvun m neliönepäjäännös.

Määritelmä 2.6 (Legendren symboli)**.** Olkoon p pariton alkuluku ja a kokonaisluku siten, että alkuluku p ei jaa sitä. Legendren symboli $\left(\frac{a}{p}\right)$ määritellään seuraavasti

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } a \text{ on luvun } p \text{ neliönjäännös} \\ -1, & \text{jos } a \text{ on luvun } p \text{ neliönepäjäännös.} \end{cases}$$

Määritelmä 2.7 (Jacobin symboli)**.** Olkoon n pariton ja positiivinen kokonaisluku siten, että sen alkulukutekijöihinjako on $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$, ja olkoon a kokonaisluku siten, että luvut a ja n ovat keskenään jaottomia. Silloin Jacobin symboli $\left(\frac{a}{n}\right)$ määritellään kaavalla

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}}\right) = \left(\frac{a}{p_1}\right)^{t_1} \left(\frac{a}{p_2}\right)^{t_2} \cdots \left(\frac{a}{p_m}\right)^{t_m},$$

missä oikeanpuoleiset symbolit ovat Legendren symboleja.

Seuraavat matriiseihin liittyvät määritelmät löytyvät Rosenin kirjasta Elementary Number Theory and Its Applications sivuilta 180-183.

Määritelmä 2.8. Kaksi kokonaislukualkioista matriisia ovat kongruentteja modulo m, jos niiden vastaavat alkiot ovat kongruentteja modulo m.

Määritelmä 2.9. (Ks. [8, s. 182]). Jos A ja $\overline{A}$ ovat $(n \times n)$ -kokonaislukumatriiseja ja kongruenssi $A\overline{A} \equiv \overline{A}A \equiv I \pmod{m}$, missä

$$I = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

on identiteettimatriisi kertalukua n, pätee, niin matriisia $\overline{A}$ kutsutaan matriisin A käänteismatriisiksi modulo m.

Määritelmä 2.10. $n \times n$-matriisin A adjungaatti on se $n \times n$-kokoinen matriisi, missä (i, j):s alkio on C_{ji}. C_{ji} muodostetaan niin, että se on $(-1)^{i+j}$ kertaa sen matriisin determinantti, joka saadaan poistamalla i:s rivi ja j:s sarake. Adjungaattia merkitään merkinnällä adj$A$.

Lause 2.14 (Eulerin kriteeri)**.** *Olkoon p pariton alkuluku ja a kokonaisluku, joka ei ole jaollinen alkuluvulla p. Silloin*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Todistus. (Vrt. [8, s. 418]). Oletetaan ensin, että $\left(\frac{a}{p}\right) = 1$. Silloin kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu $x = x_0$. Käyttämällä Fermat'n pientä lausetta nähdään, että

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \pmod{p}.$$

Siis kun $\left(\frac{a}{p}\right) = 1$, tiedetään, että $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Oletetaan seuraavaksi, että $\left(\frac{a}{p}\right) = -1$. Nyt kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole ratkaisuja. Lauseen 2.11 perusteella jokaiselle kokonaisluvulle i, kun $\text{syt}(i, p) = 1$, on olemassa kokonaisluku j siten, että $ij \equiv a \pmod{p}$. Edelleen koska kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole ratkaisuja, tiedetään, että $i \neq j$. Siis kokonaisluvut $1, 2, \ldots, p-1$ voidaan jakaa $(p-1)/2$ kappaleeseen pareja, joiden tulo on aina a. Kertomalla nämä parit keskenään huomataan, että

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}.$$

Koska Wilsonin lauseesta saadaan $(p-1)! \equiv -1 \pmod{p}$, pätee

$$-1 \equiv a^{(p-1)/2} \pmod{p}.$$

Siis myös tässä tapauksessa $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. □

2.4 Kiinalainen jäännöslause ja muita isompia apulauseita

Lause 2.15. *[Kiinalainen jäännöslause] Olkoot luvut $m_1, m_2, \ldots, m_r$ pareittain keskenään jaottomia positiivisia kokonaislukuja. Tällöin kongruenssiryhmällä*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

on yksikäsitteinen ratkaisu modulo $M = m_1 m_2 \cdots m_r$.

Todistus. (Ks. [8, s. 162-163].) Aloitetaan todistus muodostamalla yksi ratkaisu kongruenssijoukolle. Olkoon

$$M_k = M/m_k = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r.$$

Tiedetään, että $\text{syt}(M_k, m_k) = 1$, koska $\text{syt}(m_j, m_k) = 1$ aina kun $j \neq k$. Lauseen 2.8 perusteella löydetään luvun M_k käänteisluku y_k modulo m_k siten, että $M_k y_k \equiv 1 \pmod{m_k}$. Muodostetaan seuraavaksi summa

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r.$$

Kokonaisluku x on yksi ratkaisu kongruenssijoukolle. Tämän todistamiseksi näytetään ensin, että $x \equiv a_k \pmod{m_k}$ kaikilla $k = 1, 2, \ldots, r$. Koska $m_k \mid M_j$ aina, kun $j \neq k$, pätee nyt $M_j \equiv 0 \pmod{m_k}$. Nyt siis luvun x summassa kaikki termit, lukuunottamatta k. termiä, ovat kongruentteja luvun 0 kanssa modulo m_k. Näin ollen $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, koska $M_k y_k \equiv 1 \pmod{m_k}$.

Näytetään seuraavaksi, että mitkä tahansa kaksi ratkaisua ovat kongruentteja modulo M. Olkoot luvut x_0 ja x_1 vaihtoehtoisia ratkaisuja kongruenssijoukolle. Tällöin jokaisella luvulla k pätee $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$, joten $m_k \mid (x_0 - x_1)$. Lauseen 2.5 perusteella saadaan $M \mid (x_0 - x_1)$. Siis $x_0 \equiv x_1 \pmod{M}$. Tämän perusteella huomataan, että vaihtoehtoiset ratkaisut kongruenssijoukolle ovat yksikäsitteisiä modulo M. □

Lause 2.16. *[Gaussin lemma] Olkoon p pariton alkuluku ja n sellainen kokonaisluku, että* $\text{syt}(p, n) = 1$. *Merkitään luvulla r joukon $\{n, 2n, \ldots, \frac{1}{2}(p-1)n\}$ sellaisten alkioiden lukumäärää, joiden jakojäännös modulo p on suurempi kuin $p/2$. Silloin*

$$\left(\frac{n}{p}\right) = (-1)^r.$$

Todistus. (Vrt. [6, s. 138-139].) Määritellään luku s siten, että $r + s = (p-1)/2$. Käsitellään joukkoa $a_1, a_2, \ldots, a_s, b_1, b_2, \ldots, b_r$, missä $a_i < p/2$ kaikilla arvoilla i ja $b_j > p/2$ kaikilla arvoilla j. Koska kyseisen joukon alkiot ovat joukon $\{n, 2n, \ldots, \frac{1}{2}(p-1) \cdot n\}$ pienimpiä jakojäännöksiä, saadaan

$$\prod_{i=1}^{s} a_i \prod_{j=1}^{r} b_j \equiv \left(\frac{p-1}{2}\right)! n^{(p-1)/2} \pmod{p}. \tag{2.1}$$

Koska $p/2 < b_j < p$, pätee $0 < p - b_j < p/2$ kaikilla arvoilla j. Siis $a_i \neq p - b_j$ kaikilla arvoilla i ja j.

Osoitetaan seuraavaksi väitteen $a_i \neq p - b_j$ paikkansapitävyys. Tehdään vastaoletus, että $a_i = p - b_j$ joillakin arvoilla i ja j. Silloin joillakin kokonaisluvuilla h, k, missä $h \neq k$, $1 \leq h \leq (p-1)/2$, $1 \leq k \leq (p-1)/2$, pätee

$$(h + k)n \equiv hn + kn \equiv a_i + b_j \equiv p \equiv 0 \pmod{p}.$$

Tästä seuraa, että $p \mid (h + k)n$ ja koska $\text{syt}(p, n) = 1$, niin $p \mid (h + k)$. Kuitenkaan tämä ei voi pitää paikkaansa, koska $0 < h + k < p$.

Edellisistä ehdoista seuraa, että kaikki $(p-1)/2$ kokonaislukua $a_1, a_2, \ldots, a_s, p - b_1, \ldots, p - b_r$, ovat erisuuria ja toteuttavat epäyhtälön $1 \leq x \leq (p-1)/2$. Siis ne ovat kokonaisluvut $1, 2, \ldots, (p-1)/2$ jossain järjestyksessä. Nyt siis

$$\left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{s} a_i \prod_{j=1}^{r} (p - b_j) \pmod{p}.$$

Nyt p voidaan hävittää kongruenssista, koska käsitellään kongruenssia modulo p. Siis

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^r \prod_{i=1}^{s} a_i \prod_{j=1}^{r} b_j \pmod{p}.$$

Käyttämällä yhtälöä (2.1) saadaan

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^r \left(\frac{p-1}{2}\right)! n^{(p-1)/2} \pmod{p}. \tag{2.2}$$

Koska $\left(\frac{p-1}{2}\right)!$ ja p ovat selvästi keskenään jaottomia, voidaan kongruenssin (2.2) molemmat puolet jakaa luvulla $\left(\frac{p-1}{2}\right)!$.

Edeltävistä ehdoista seuraa, että

$$1 \equiv (-1)^r n^{(p-1)/2} \pmod{p}. \tag{2.3}$$

Kertomalla yhtälön (2.3) molemmat puolet luvulla $(-1)^r$ ja käyttämällä Eulerin kriteeriä saadaan

$$(-1)^r \equiv n^{(p-1)/2} \equiv \left(\frac{n}{p}\right) \pmod{p}. \tag{2.4}$$

Siis $(-1)^r - \left(\frac{n}{p}\right) = tp$ jollain luvulla t. Mutta koska yhtälön vasemman puolen tulee olla ± 2 tai 0 Legendren symbolin $\left(\frac{n}{p}\right)$ määritelmän $\left(\frac{n}{p}\right) = \pm 1$ mukaan seuraa, että $t = 0$, josta edelleen seuraa $\left(\frac{n}{p}\right) = (-1)^r$. □

Lause 2.17. *[Resiprookkilause] Jos luvut p ja q ovat erisuuria parittomia alkulukuja, niin*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

Todistus. (Vrt. [6, s. 139-141].) Todistus perustuu ylläesitettyyn Gaussin lemmaan. Käsitellään kokonaislukuja $q, 2q, ..., \frac{1}{2}(p-1)q$. Olkoon $1 \leq k \leq (p-1)/2$. Jakoalgoritmin perusteella $kq = pq_k + t_k$, kun q_k ja t_k ovat kokonaislukuja siten, että $1 \leq t_k \leq p-1$. Siis t_k on pienin luvun kq jakojäännös mod p. Koska $kq = pq_k + t_k$, missä $0 \leq t_k < p$, pätee

$$\frac{kq}{p} = q_k + \frac{t_k}{p},$$

joten $0 \leq t_k/p < 1$. Nyt siis $q_k = \lfloor kq/p \rfloor$. Merkitään symboleilla $a_1, a_2, ..., a_s$ luvun t_k niitä arvoja, jotka ovat pienempiä kuin $p/2$, ja merkitään symboleilla $b_1, b_2, ..., b_s$ luvun t_k niitä arvoja, jotka ovat suurempia kuin $p/2$. Siis Gaussin lemman perusteella $\left(\frac{q}{p}\right) = (-1)^r$.

Olkoon $a = \sum_{i=1}^{s} a_i$ ja $b = \sum_{j=1}^{r} b_j$ joten

$$a + b = \sum_{i=1}^{s} a_i + \sum_{j=1}^{r} b_j = \sum_{k=1}^{(p-1)/2} t_k. \tag{2.5}$$

Kuten Gaussin lemman todistuksessa luvut $a_1, ..., a_s, p - b_1, ..., p - b_r$ ovat luvut $1, 2, ..., (p-1)/2$ jossain järjestyksessä. Siis

$$\begin{aligned} a + rp - b &= \sum_{i=1}^{s} a_i + \sum_{j=1}^{r} (p - b_j) \\ &= \sum_{k=1}^{(p-1)/2} k. \end{aligned} \tag{2.6}$$

Käytetään seuraavaksi kaavaa $\sum_{k=0}^{n} k = \frac{1}{2}n(n+1)$, mihin sijoitetaan $n = (p-1)/2$ ja saadaan

$$a + rp - b = \sum_{k=1}^{(p-1)/2} k = \frac{p^2-1}{8}. \tag{2.7}$$

Yhdistämällä yhtälöt $kq = pq_k + t_k$ ja (2.5) saadaan

$$p \sum_{k=1}^{(p-1)/2} q_k + a + b = \sum_{k=1}^{(p-1)/2} (pq_k + t_k) \tag{2.8}$$

$$= \sum_{k=1}^{(p-1)/2} kq. \tag{2.9}$$

Käytetään vielä yhtälöä (2.6), jolloin saadaan

$$p \sum_{k=1}^{(p-1)/2} q_k + a + b = \frac{p^2-1}{8} \cdot q. \tag{2.10}$$

Vähentämällä yhtälö (2.6) yhtälöstä (2.10) puolittain saadaan

$$p \sum_{k=1}^{(p-1)/2} q_k + 2b - rp = \frac{p^2-1}{8} \cdot (q-1). \tag{2.11}$$

Käytetään seuraavaksi hyväksi sitä tietoa, että luku q on pariton. Tavoitteena on selvittää, mikä lausekkeen $(-1)^r$ arvo on, ja siksi halutaan tietää, kumpi seuraavista kongruensseista pitää paikkansa $r \equiv 0$ vai $r \equiv 1 \pmod 2$. Koska $(p^2-1)/8$ on kokonaisluku, ja $p \equiv q \equiv 1 \pmod 2$, yhtälöstä (2.11) saadaan seuraava kongruenssi

$$\sum_{k=1}^{(p-1)/2} q_k \equiv r \pmod 2. \tag{2.12}$$

Merkitään seuraavaksi

$$u = \sum_{k=1}^{(p-1)/2} q_k = \sum_{k=1}^{(p-1)/2} \lfloor kq/p \rfloor.$$

Nyt kongruenssin (2.12) ja Gaussin lemman perusteella saadaan

$$\left(\frac{q}{p}\right) = (-1)^r = (-1)^u.$$

Jos toistetaan sama käsittely, mutta vaihdetaan lukujen p ja q paikkoja ja merkitään

$$v = \sum_{k=1}^{(q-1)/2} \lfloor jp/q \rfloor,$$

saadaan $\left(\frac{p}{q}\right) = (-1)^v$. Siis

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{u+v}.$$

Seuraavaksi täytyy vielä osoittaa, että seuraava väite pätee:

$$u + v = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1).$$

Olkoon T sellainen joukko, joka koostuu muotoa $jp - kq$ olevista alkioista, kun $k = 1, 2, .., \frac{1}{2}(p-1)$ ja $j = 1, 2, ..., \frac{1}{2}(q-1)$. Todistetaan, että mikään joukon T alkioista ei ole nolla. Nimittäin jos olisi $jp - kq = 0$, niin $jp = kq$ ja $p \mid kq$. Mutta tämä ei voi pitää paikkaansa, koska syt$(p, q) = 1$ ja $1 \leq k \leq (p-1)/2$. Sama perustelu pätee väitteelle, että kaikki joukon T alkiot ovat erisuuria ja T sisältää $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ alkiota.

Seuraavaksi tutkitaan, kuinka monta positiivista ja negatiivista alkiota joukossa T on. Jokaiselle alkiolle j, $jp - kq > 0$ kaikilla arvoilla $k = 1, 2, ..., x$, missä x on suurin kokonaisluku siten, että $jp > xq$. Siis jokaista luvun j arvoa kohti on olemassa $x = \lfloor jp/q \rfloor$ arvoa luvulle k, jotka tuottavat positiivisia joukon T alkioita. Siis joukon T positiivisten alkioiden kokonaismäärä on

$$v = \sum_{k=1}^{(q-1)/2} \lfloor jp/q \rfloor.$$

Samoin,

$$u = \sum_{k=1}^{(p-1)/2} \lfloor kq/q \rfloor$$

on joukon T negatiivisten arvojen lukumäärä. Näin käydään läpi joukon T alkiot ja saadaan

$$u + v = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1).$$

□

3 Pseudoalkuluvuista

3.1 Pseudoalkulukujen määritelmä

Fermat'n pieni lause kertoo, että jos n on alkuluku ja b on mikä tahansa kokonaisluku, niin $b^n \equiv b \pmod{n}$. Toisaalta siis, jos löydetään kokonaisluku b siten, että $b^n \not\equiv b \pmod{n}$, niin tiedetään, että n on yhdistetty luku.

Esimerkki 3.1. Voidaan näyttää, että luku 15 ei ole alkuluku käyttämällä Fermat'n pientä lausetta:

$$2^{15} = 2^{12} \cdot 2^3 = (2^4)^3 \cdot 2^3 = 16^3 \cdot 2^3 \equiv 2^3 \equiv 8 \not\equiv 2 \pmod{15}.$$

Fermat'n pienen lauseen avulla voidaan siis näyttää, että luku on yhdistetty luku. Olisi vielä hienompaa, jos sen avulla voitaisiin näyttää, että kokonaisluku on alkuluku. Aiemmin luultiin, että jos $2^n \equiv 2 \pmod{n}$, niin luvun n tulee olla alkuluku. Tämä väite pätee luvuilla $1 \leq n \leq 340$. Valitettavasti käänteinen Fermat'n pieni lause ei päde, kuten seuraava esimerkki todistaa. Esimerkin $n = 341$ keksi Sarrus vuonna 1919.

Esimerkki 3.2. Olkoon $n = 561 = 3 \cdot 11 \cdot 17$. Fermat'n pienen lauseen perusteella nähdään, että

$$\begin{aligned} 2^{560} &= (2^2)^{280} \equiv 1 \pmod{3}, \\ 2^{560} &= (2^{10})^{56} \equiv 1 \pmod{11}, \\ 2^{560} &= (2^{16})^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Siis lauseen 2.6 nojalla saadaan, että $2^{560} \equiv 1 \pmod{561}$. Kertomalla kongruenssin molemmat puolet luvulla 2 saadaan

$$2^{561} \equiv 2 \pmod{561},$$

vaikka luku 561 ei ole alkuluku.

Tämänkaltaiset esimerkit johtivat seuraavaan määritelmään.

Määritelmä 3.1. Olkoon b positiivinen kokonaisluku. Jos n on yhdistetty ja positiivinen kokonaisluku sekä $b^n \equiv b \pmod{n}$, niin lukua n kutsutaan pseudoalkuluvuksi kannan b suhteen.

Huomataan, että jos $\text{syt}(b, n) = 1$, niin kongruenssi $b^n \equiv b \pmod{n}$ on ekvivalentti kongruenssin $b^{n-1} \equiv 1 \pmod{n}$ kanssa. Ensimmäisestä kongruenssista saadaan toinen jakamalla molemmat puolet luvulla b ja ensimmäinen kongruenssi saadaan toisesta kertomalla molemmat puolet luvulla b.

Jos on olemassa suhteellisen vähän pseudoalkulukuja kannan b suhteen, kongruenssin $b^n \equiv b \pmod{n}$ tarkastelu on hyödyllinen testi. Ainoastaan pieni määrä jaollisia

lukuja läpäisee testin. Itse asiassa on olemassa paljon vähemmän pseudoalkuluja kannan b suhteen tiettyyn lukuun asti kuin alkulukuja. Esimerkiksi on olemassa 455 052 512 alkulukua ja 14 884 pseudoalkulukua kannan b suhteen, mitkä ovat lukua 10^{10} pienempiä. Vaikka pseudoalkuluvut ovatkin harvinaisia, on niitä silti olemassa ääretön määrä jokaisen kannan suhteen.

Apulause 3.1. Jos d ja n ovat positiivisia kokonaislukuja siten, että $d \mid n$, niin

$$(2^d - 1) \mid (2^n - 1).$$

Todistus. (Ks. [8, s. 226].) Koska $d \mid n$, on olemassa positiivinen kokonaisluku t siten, että $dt = n$. Merkitään $x = 2^d$ yhtälössä $x^t - 1 = (x - 1)(x^{t-1} + x^{t-2} + \cdots + 1)$, eli

$$2^n - 1 = (2^d - 1)(2^{d(t-1)} + 2^{d(t-2)} + \cdots + 2^d + 1).$$

Nyt siis $(2^d - 1) \mid (2^n - 1)$. □

Lause 3.2. *On olemassa ääretön määrä pseudoalkulukuja kannan* 2 *suhteen.*

Todistus. (Ks. [8, s. 226-227].) Osoitetaan, että jos n on pariton pseudoalkuluku kannan 2 suhteen, niin myös $m = 2^n - 1$ on pariton pseudoalkuluku kannan 2 suhteen. Koska on olemassa ainakin yksi pariton pseudoalkuluku kannan 2 suhteen, nimittäin $n_0 = 341$, voidaan muodostaa ääretön määrä parittomia pseudoalkulukuja kannan 2 suhteen merkitsemällä $n_0 = 341$ ja $n_{k+1} = 2^{n_k} - 1$, kun $k = 0, 1, 2, 3, \ldots$. Kaikki näin muodostetut kokonaisluvut ovat eri lukuja, sillä

$$n_0 < n_1 < n_2 < \cdots < n_k < n_{k+1} < \cdots.$$

Oletetaan seuraavaksi, että n on pariton pseudoalkuluku kannan 2 suhteen, eli n on yhdistetty luku ja $2^{n-1} \equiv 1 \pmod{n}$. Koska n on yhdistetty luku, voidaan merkitä $n = dt$, missä $1 < d < n$ ja $1 < t < n$. Osoitetaan nyt, että $m = 2^n - 1$ on myös pseudoalkuluku näyttämällä ensin, että se on yhdistetty luku ja sitten että kongruenssi $2^{m-1} \equiv 1 \pmod{m}$ pätee.

Luvun m jaollisuuden todistamiseksi käytetään lausetta 3.1 osoittamaan, että $(2^d - 1) \mid (2^n - 1) = m$. Koska $2^n \equiv 2 \pmod{n}$, huomataan, että on olemassa kokonaisluku k siten, että $2^n - 2 = kn$. Siis $2^{m-1} = 2^{2^n-2} = 2^{kn}$. Apulauseen 3.1 avulla nähdään, että

$$m = (2^n - 1) \mid (2^{kn} - 1) = 2^{m-1} - 1.$$

Nyt siis $2^{m-1} - 1 \equiv 0 \pmod{m}$, joten $2^{m-1} \equiv 1 \pmod{m}$. Tästä nähdään, että m on pseudoalkuluku kannan 2 suhteen. □

Jos halutaan tietää, onko kokonaisluku n alkuluku ja huomataan, että kongruenssi $2^{n-1} \equiv 1 \pmod{n}$ pätee, niin n on joko alkuluku tai pseudoalkuluku kannan 2 suhteen. Asian selvittämisen jatkamiseksi voidaan testata kongruenssia $b^{n-1} \equiv 1 \pmod{n}$ monilla positiivisilla kokonaisluvuilla b. Jos löydetään luvun b arvoja siten, että $\text{syt}(b, n) = 1$ ja $b^{n-1} \not\equiv 1 \pmod{n}$, tiedetään, että n on yhdistetty luku.

Esimerkki 3.3. (Ks. [8, s. 227].) Näytetään ensin, että 341 on pseudoalkuluku kannan 2 suhteen:

$$2^{341} = 2^{340} \cdot 2 = (2^{10})^{34} \cdot 2 = 1024^{34} \cdot 2 \equiv 1^{34} \cdot 2 \equiv 2 \pmod{341}.$$

Koska

$$7^3 = 343 \equiv 2 \pmod{341}$$

ja

$$2^{10} = 1024 \equiv 1 \pmod{341},$$

saadaan

$$\begin{aligned} 7^{340} =& (7^3)^{113} \cdot 7 \equiv 2^{113} \cdot 7 = (2^{10})^{11} \cdot 2^3 \cdot 7 \\ \equiv& 8 \cdot 7 \equiv 56 \not\equiv 1 \pmod{341}. \end{aligned}$$

Käyttämällä Fermat'n pientä lausetta käännettynä nähdään, että 341 on yhdistetty luku, koska $7^{340} \not\equiv 1 \pmod{341}$.

3.2 Carmichaelin luvut

Valitettavasti on olemassa jaollisia kokonaislukuja n siten, että niitä ei pystytä osoittamaan jaollisiksi käyttämällä yllä olevaa tapaa. Näin on, koska on olemassa kokonaislukuja, jotka ovat pseudoalkulukuja jokaisen kannan suhteen, eli on olemassa jaollisia kokonaislukuja n siten, että $b^{n-1} \equiv 1 \pmod{n}$ kaikilla luvuilla b kun $\text{syt}(b, n) = 1$. Tämä johtaa seuraavaan määritelmään, joka on nimetty Robert Carmichaelin mukaan. Carmichael tutki asiaa 1900-luvun alkupuolella.

Määritelmä 3.2. Yhditettyä kokonaislukua n, joka toteuttaa kongruenssin $b^{n-1} \equiv 1 \pmod{n}$ kaikilla sellaisilla positiivisilla kokonaisluvuilla b, että $\text{syt}(b, n) = 1$, kutsutaan Carmichaelin luvuksi tai absoluuttiseksi pseudoalkuluvuksi.

Esimerkki 3.4. Kokonaisluku $1105 = 5 \cdot 13 \cdot 17$ on Carmichaelin luku. Todetaan aluksi, että jos $\text{syt}(b, 1105) = 1$, niin myös

$$\text{syt}(b, 5) = \text{syt}(b, 13) = \text{syt}(b, 17) = 1.$$

Fermat'n pienen lauseen perusteella voidaan muodostaa kongruenssit $b^4 \equiv 1 \pmod{5}$, $b^{12} \equiv 1 \pmod{13}$ ja $b^{16} \equiv 1 \pmod{17}$. Siis

$$\begin{aligned} b^{1104} &= (b^4)^{276} \equiv 1 \pmod{5}, \\ b^{1104} &= (b^{12})^{92} \equiv 1 \pmod{13}, \\ b^{1104} &= (b^{16})^{69} \equiv 1 \pmod{17}. \end{aligned}$$

Nyt siis lauseen 2.6 perusteella $b^{1104} \equiv 1 \pmod{1105}$ kaikilla b, kun $\text{syt}(b, n) = 1$. Siis 1105 on Carmichaelin luku.

Lause 3.3. *Olkoon n on yhdistetty kokonaisluku. Jos n on jaollinen jollain täydellisellä neliöllä, n ei ole Carmichaelin luku.*

Todistus. (Vrt. [2, s. 1].) Oletetaan, että n on Carmichaelin luku. Todistetaan, että luku n ei ole jaollinen millään neliöllä. Jos alkuluvun p potenssi > 1 jakaa luvun n, merkitään $n = p^k n'$, missä $k \geq 1$ ja $\text{syt}(p, n') = 1$. Tavoitteena on nyt osoittaa, että $k = 1$.

Tehdään vastaoletus, että $k \geq 2$, joten $p^2 \mid n$. Kiinalaisen jäännöslauseen mukaan on olemassa kokonaisluku a siten, että $a \equiv 1 + p \pmod{p^k}$ ja $a \equiv 1 \pmod{n'}$. Nyt siis $\text{syt}(a, n) = 1$, joten Carmichaelin lukujen määritelmän mukaan

$$a^{n-1} \equiv 1 \pmod{n}.$$

Nyt koska $p^2 \mid n$ ja $a \equiv 1 + p \pmod{p^k}$, niin edellä olevasta kongruenssista seuraa, että

$$(1 + p)^{n-1} \equiv 1 \pmod{p^2}.$$

Binomilauseen mukaan pätee

$$(1 + p)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} p^i \equiv 1 + (n-1)p \pmod{p^2}.$$

Nyt koska $p \mid n$, saadaan

$$1 + (n-1)p \equiv 1 + np - p \equiv 1 - p \pmod{p^2}.$$

Siis

$$1 - p \equiv 1 \pmod{p^2}.$$

Tämä ei voi päteä, joten tulos on ristiriita ja $k = 1$. □

Vuonna 1912 Carmichael väitti, että on olemassa äärettömän monta Carmichaelin lukua. Kesti 80 vuotta, että väite pystyttiin todistamaan. Vuonna 1992 Alford, Granville ja Pomerance todistivat, että Carmichael oli oikeassa. Seuraavaksi esitetään osa kyseisestä todistuksesta; teoreema, jolla voidaan löytää Carmichaelin lukuja.

Lause 3.4. *Olkoon n pariton yhdistetty kokonaisluku. Jos mikään neliö ei jaa lukua n, on n Carmichaelin luku, jos ja vain jos $p - 1 \mid n - 1$ jokaisella luvulla p, joka jakaa luvun n.*

Todistus. (Ks. [4, s. 128].) □

Esimerkki 3.5. Lauseen 3.4 nojalla $8911 = 7 \cdot 19 \cdot 67$ on Carmichaelin luku, koska kaikki luvut 7, 19, 67 ovat alkulukuja ja $6 = (7-1) \mid 8910$, $18 = (19-1) \mid 8910$ sekä $66 = (67-1) \mid 8910$.

3.3 Millerin testi

Kun kongruenssi $b^{n-1} \equiv 1 \pmod{n}$, missä n on pariton kokonaisluku, on testattu, toinen mahdollinen lähestymistapa on tutkia luvun $b^{(n-1)/2}$ pienintä jäännöstä modulo n. Nythän jos $x = b^{(n-1)/2}$, niin $x^2 = b^{n-1} \equiv 1 \pmod{n}$. Jos n on alkuluku, niin lauseen 2.1 perusteella tiedetään, että joko $x \equiv 1$ tai $x \equiv -1 \pmod{n}$. Kun ensin todetaan, että $b^{n-1} \equiv 1 \pmod{n}$, voidaan kokeilla kongruenssia $b^{(n-1)/2} \equiv \pm 1 \pmod{n}$. Jos edellä oleva kongruenssi ei päde, tiedetään, että n on yhdistetty luku.

Esimerkki 3.6. Olkoon $b = 5$ ja $n = 1105$. Huomataan, että $5^{(1105-1)/2} = 5^{552} \equiv 560 \pmod{1105}$ eli luku 1105 on yhdistetty luku.

Määritelmä 3.3. Olkoon n positiivinen kokonaisluku. Merkitään $n-1 = 2^s t$, missä s on ei-negatiivinen kokonaisluku ja t on pariton positiivinen kokonaisluku. Sanotaan, että luku n toteuttaa Millerin testin kannalle b, jos joko $b^t \equiv 1 \pmod{n}$ tai $b^{2^j t} \equiv -1 \pmod{n}$ jollakin luvulla j, kun $0 \leq j \leq s-1$.

Esimerkki 3.7. Olkoon $n = 121 = 11^2$. Nyt

$$3^{120} = (3^5)^{24} = 243^{24} \equiv 1 \pmod{121},$$

joten 121 on pseudoalkuluku kannan 3 suhteen.

Nyt merkitään, että $121-1 = 120 = 2^4 \cdot 15$ ja Millerin testin määritelmän mukaan

$$3^{15} = (3^5)^3 = 243^3 \equiv 1^3 \equiv 1 \pmod{121},$$

eli 121 toteuttaa Millerin testin kannalle 3.

Lause 3.5. *Jos n on alkuluku ja b on positiivinen kokonaisluku siten, että $n \nmid b$, niin luku n toteuttaa Millerin testin kannalle b.*

Todistus. (Ks. [8, s. 229].) Olkoon $n-1 = 2^s t$, missä s on ei-negatiivinen kokonaisluku ja t on pariton ja positiivinen kokonaisluku. Olkoon $x_k = b^{(n-1)/2^k} = b^{2^{s-k}t}$, kun $k = 0, 1, 2, \ldots, s$. Koska n on alkuluku, Fermat'n pienen lauseen perusteella tiedetään, että $x_0 = b^{n-1} \equiv 1 \pmod{n}$. Lauseen 2.1 perusteella koska $x_1^2 = (b^{(n-1)/2})^2 = x_0 \equiv 1 \pmod{n}$, niin $x_1 \equiv -1 \pmod{n}$ tai $x_1 \equiv 1 \pmod{n}$. Jos $x_1 \equiv 1 \pmod{n}$, koska $x_2^2 = x_1 \equiv 1 \pmod{n}$, niin $x_2 \equiv -1 \pmod{n}$ tai $x_2 \equiv 1 \pmod{n}$. Jos

$$x_0 \equiv x_1 \equiv x_2 \equiv x_3 \equiv \cdots \equiv x_k \equiv 1 \pmod{n},$$

missä $k < s$, niin koska $x_{k+1}^2 = x_k \equiv 1 \pmod{n}$, tiedetään, että joko $x_{k+1} \equiv -1 \pmod{n}$ tai $x_{k+1} \equiv 1 \pmod{n}$.

Kun tätä jatketaan $k = 1, 2, 3, \ldots, s$, huomataan, että joko $x_k \equiv 1 \pmod{n}$ tai $x_k \equiv -1 \pmod{n}$ jollakin kokonaisluvulla k, missä $0 < k \leq s$. Siis luku n toteuttaa Millerin testin kannalle b. □

Olkoon $n-1 = 2^s t$ ja luku t pariton. Jos positiivinen kokonaisluku n toteuttaa Millerin testin kannalle b, niin $b^t \equiv 1 \pmod{n}$ tai $b^{2^j t} \equiv -1 \pmod{n}$ jollakin luvulla j, missä $0 \leq j \leq s-1$.

Kummassakin tapauksessa saadaan $b^{n-1} \equiv 1 \pmod{n}$, koska $b^{n-1} = (b^{2^j t})^{2^{s-1}} \equiv 1 \pmod{n}$, kun $j = 0, 1, 2, \ldots, s$, eli siis yhdistetty luku joka toteuttaa Millerin testin kannalle b on automaattisesti pseudoalkuluku kannan b suhteen.

3.4 Vahvat pseudoalkuluvut

Määritelmä 3.4. Jos n on yhdistetty luku ja toteuttaa Millerin testin kannan b suhteen, niin sanotaan, että b on vahva pseudoalkuluku kannan b suhteen.

Esimerkki 3.8. Nyt huomataan, että esimerkin 3.7 luku 121 on äskeisen määritelmän perusteella myös vahva pseudoalkuluku kannan 3 suhteen.

Vaikka vahvat pseudoalkuluvut ovat äärimmäisen harvinaisia, on niitä silti olemassa ääretön määrä. Annetaan seuraavaksi esimerkkinä äärettömyyden todistus kannalle 2.

Lause 3.6. *On olemassa ääretön määrä vahvoja pseudoalkulukuja kannan* 2 *suhteen.*

Todistus. (Ks. [8, s. 230].) Tavoitteena on osoittaa, että jos n on pseudoalkuluku kannan 2 suhteen, niin $N = 2^n - 1$ on vahva pseudoalkuluku kannan 2 suhteen.

Olkoon n pariton kokonaisluku siten, että se on pseudoalkuluku kannan 2 suhteen. Siis n on yhdistetty luku ja $2^{n-1} \equiv 1 \pmod{n}$. Tämän kongruenssin perusteella saadaan, että $2^{n-1} - 1 = nk$ jollakin kokonaisluvulla k. Lisäksi luvun k tulee olla pariton. Nyt

$$N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2^1 nk.$$

Huomataan, että

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \pmod{N},$$

koska $2^n = (2^n - 1) + 1 = N + 1 \equiv 1 \pmod{N}$. Tämän perusteella tiedetään, että luku N toteuttaa Millerin testin kannalle 2.

Lauseen 3.1 todistuksessa osoitettiin, että jos luku n on yhdistetty, niin luku $N = 2^n - 1$ on myös yhdistetty. Eli nyt luku N toteuttaa Millerin testin ja on yhdistetty, joten N on vahva pseudoalkuluku kannan 2 suhteen. Koska jokaista pseudoalkulukua n kannan 2 suhteen vastaa vahva pseudoalkuluku $2^n - 1$ kannan 2 suhteen, ja koska on olemassa ääretön määrä pseudoalkulukuja kannan 2 suhteen, on olemassa ääretön määrä vahvoja pseudoalkulukuja kannan 2 suhteen. □

3.5 Eulerin pseudoalkuluvut

Olkoon p pariton alkuluku ja b kokonaisluku, joka ei ole jaollinen luvulla p. Eulerin kriteerin perusteella tiedetään, että

$$b^{(p-1)/2} \equiv \left(\frac{b}{p}\right) \pmod{p}.$$

Jos halutaan ottaa selvää, onko positiivinen kokonaisluku n alkuluku, voidaan ottaa käsittelyyn luku b siten, että $\mathrm{syt}(b, n) = 1$, ja testata päteekö

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n},$$

missä kongruenssin oikeanpuoleinen merkintä on Jacobin symboli. Jos kongruenssi ei päde, on luku n yhdistetty.

Määritelmä 3.5. Paritonta, jaollista ja positiivista kokonaislukua n, joka toteuttaa kongruenssin

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n},$$

missä b on positiivinen kokonaisluku, kutsutaan Eulerin pseudoalkuluvuksi kannan b suhteen.

Esimerkki 3.9. Olkoon $n = 561$ ja $b = 2$. Nyt $2^{280} \equiv 1 \pmod{561}$. Nyt lasketaan Jacobin symboli

$$\left(\frac{2}{1105}\right) = \left(\frac{2}{3 \cdot 11 \cdot 17}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{11}\right)\left(\frac{2}{17}\right) = (-1) \cdot (-1) \cdot 1 = 1.$$

Siis $2^{280} \equiv \left(\frac{2}{561}\right) \pmod{561}$. Koska luku 561 on yhdistetty ja pariton, on se Eulerin pseudoalkuluku kannan 2 suhteen.

Seuraava lause osoittaa, että jokainen Eulerin pseudoalkuluku kannan b suhteen on myös pseudoalkuluku kannan b suhteen.

Lause 3.7. *Jos luku n on Eulerin pseudoalkuluku kannan b suhteen, niin n on pseudoalkuluku kannan b suhteen.*

Todistus. (Ks. [8, s. 454].) Jos n on Eulerin pseudoalkuluku kannan b suhteen, niin

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Korotetaan kongruenssin molemmat puolet toiseen potenssiin ja saadaan

$$(b^{(n-1)/2})^2 \equiv \left(\frac{b}{n}\right)^2 \pmod{n}.$$

Koska $\left(\frac{b}{n}\right) = \pm 1$, saadaan

$$b^{n-1} \equiv 1 \pmod{n},$$

mistä seuraa, että n on pseudoalkuluku kannan b suhteen. □

Lause 3.8. *Olkoot a, d ja r positiivisia kokonaislukuja. Nyt kongruenssi*

$$(2^{r+1}d + 1)^a \equiv (1 + 2^{r+1}ad) \pmod{2^{2r+2}}$$

pätee.

Todistus. Todistetaan kongruenssin pätevyys induktiolla luvun a suhteen.

1. Olkoon $a = 1$. Nyt

$$(2^{r+1}d + 1)^1 \equiv 1 + 2^{r+1} \cdot 1 \cdot d \pmod{2^{2r+2}}.$$

2. Oletetaan, että kongruenssi pätee, kun $a = n$:

$$(2^{r+1}d + 1)^n \equiv (1 + 2^{r+1}nd) \pmod{2^{2r+2}}.$$

3. Osoitetaan seuraavaksi, että kongruenssi pätee, kun $a = n + 1$. Nyt

$$\begin{aligned}
(2^{r+1}d + 1)^{n+1} &\equiv (1 + 2^{r+1}(n+1)d) \pmod{2^{2r+2}} \\
\Leftrightarrow (2^{r+1}d + 1)(2^{r+1} + 1)^n &\equiv (1 + 2^{r+1}(n+1)d) \pmod{2^{2r+2}} \\
\Leftrightarrow (2^{r+1}d + 1)(1 + 2^{r+1}nd) &\equiv (1 + 2^{r+1}(n+1)d) \pmod{2^{2r+2}} \\
\Leftrightarrow 2^{r+1}d + 2^{2r+2}2nd + 1 + 2^{r+1}nd &\equiv 1 + 2^{r+1}nd + 2^{r+1}d \pmod{2^{2r+2}} \\
\Leftrightarrow 2^{r+1}d + 1 + 2^{r+1}nd &\equiv 1 + 2^{r+1}nd + 2^{r+1}d \pmod{2^{2r+2}} \\
\Leftrightarrow 1 &\equiv 1 \pmod{2^{2r+2}}.
\end{aligned}$$

□

Lause 3.9. *Jos n on vahva pseudoalkuluku kannan b suhteen, niin n on Eulerin pseudoalkuluku kannan b suhteen.*

Todistus. (Vrt. [8, s. 454-456].) Olkoon n vahva pseudoalkuluku kannan b suhteen. Nyt jos $n - 1 = 2^s t$, missä luku t on pariton, silloin

$$b^t \equiv 1 \pmod{n} \quad \text{tai} \quad b^{2^r t} \equiv -1 \pmod{n},$$

missä $0 \leq r \leq s - 1$. Olkoon $n = \prod_{i=1}^{m} p_i^{a_i}$ luvun n alkulukutekijöihinjako.

Käsitellään aluksi tapausta $b^t \equiv 1 \pmod{n}$. Olkoon p luvun n alkulukutekijä. Nyt lauseen 2.13 mukaan koska $b^t \equiv 1 \pmod{p}$, niin $\operatorname{ord}_p b \mid t$. Koska luku t on pariton, niin luvun t tekijänä myös $\operatorname{ord}_p b$ on pariton. Siis $\operatorname{ord}_p b \mid (p-1)/2$, koska $\operatorname{ord}_p b$ on parillisen luvun $\phi(p) = p - 1$ pariton jakaja. Tästä seuraa, että

$$b^{(p-1)/2} \equiv 1 \pmod{p}.$$

Edelleen Eulerin kriteerin (lause 2.14) perusteella saadaan, että $\left(\frac{b}{p}\right) = 1$.

Lasketaan seuraavaksi Jacobin symboli $\left(\frac{b}{n}\right)$. Edellä on todistettu, että $\left(\frac{b}{p}\right) = 1$ kaikilla alkuluvuilla p, jotka jakavat luvun n. Siis

$$\left(\frac{b}{n}\right) = \left(\frac{b}{\prod_{i=1}^{m} p_i^{a_i}}\right) = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{a_i} = 1.$$

Koska $b^t \equiv 1 \pmod{n}$, tiedetään, että $b^{(n-1)/2} = (b^t)^{2^{s-1}} \equiv 1 \pmod{n}$. Tästä seuraa, että

$$b^{(n-1)/2} \equiv 1 \equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Siis n on Eulerin pseudoalkuluku kannan b suhteen.

Seuraavaksi otetaan käsittelyyn tapaus

$$b^{2^r t} \equiv -1 \pmod{n}$$

jollain luvulla r, kun $0 \leq r \leq s-1$. Jos p on luvun n alkulukujakaja, niin

$$b^{2^r t} \equiv -1 \pmod{p}.$$

Korottamalla molemmat puolet toiseen potenssiin saadaan

$$b^{2^{r+1} t} \equiv 1 \pmod{p},$$

mistä seuraa, että $\mathrm{ord}_p b \mid 2^{r+1}t$, mutta myös että $\mathrm{ord}_p b \nmid 2^r t$. Siis

$$\mathrm{ord}_p b = 2^{r+1}c,$$

missä c on pariton kokonaisluku. Koska $\mathrm{ord}_p b \mid (p-1)$ ja $2^{r+1} \mid \mathrm{ord}_p b$, siitä seuraa, että $2^{r+1} \mid (p-1)$. Nyt siis $p = 2^{r+1}d + 1$, missä d on kokonaisluku. Koska $\mathrm{ord}_p\, b = 2^{r+1}c$, niin

$$(b^{2^r c})^2 \equiv 1 \pmod{p},$$

siis $b^{2^r c} \equiv 1 \pmod{p}$ tai $b^{2^r c} \equiv -1 \pmod{p}$. Koska $2^r c = (\mathrm{ord}_p\, b)/2$, niin

$$b^{2^r c} \not\equiv 1 \pmod{p}.$$

Siis

$$b^{2^r c} \equiv -1 \pmod{p}$$

eli

$$b^{(\mathrm{ord}_p b)/2} \equiv -1 \pmod{n},$$

joten saadaan Eulerin kriteerin avulla

$$\begin{aligned}\left(\frac{b}{p}\right) &\equiv b^{(p-1)/2} = b^{(ord_p b/2)((p-1)/ord_p b)} \\ &\equiv (-1)^{(p-1)/ord_p b} = (-1)^{(p-1)/(2^{r+1}c)} \pmod{p}.\end{aligned}$$

Koska luku c on pariton, tiedetään, että $(-1)^c = -1$. Siis

$$\left(\frac{b}{p}\right) = (-1)^{(p-1)/2^{r+1}} = (-1)^d, \tag{3.1}$$

koska $d = (p-1)/2^{r+1}$. Koska jokainen alkuluku p_i, joka jakaa luvun n, on muotoa

$p_i = 2^{r+1}d_i + 1$, seuraa siitä, että

$$\begin{aligned}
n &= \prod_{i=1}^{m} p_i^{a_i} \\
&= \prod_{i=1}^{m} (2^{r+1}d_i + 1)^{a_i} \\
&\overset{*}{\equiv} \prod_{i=1}^{m} (1 + 2^{r+1}a_i d_i) \\
&\equiv (1 + 2^{r+1}a_1 d_1) \cdot (1 + 2^{r+1}a_2 d_2) \cdot (1 + 2^{r+1}a_3 d_3) \cdots \\
&\equiv (1 + 2^{r+1}a_1 d_1 + 2^{r+1}a_2 d_2 + 2^{2r+2}a_1 a_2 d_1 d_2 + 2^{r+1}a_3 d_3 \\
&\qquad + 2^{2r+2}a_1 a_3 d_1 d_3 + 2^{2r+2}a_2 a_3 d_2 d_3 + 2^{3r+3}a_1 a_2 a_3 d_1 d_2 d_3) \cdots \\
&\equiv (1 + 2^{r+1}a_1 d_1 + 2^{r+1}a_2 d_2 + 2^{r+1}a_3 d_3) \cdots \\
&\equiv 1 + 2^{r+1} \sum_{i=1}^{m} a_i d_i \pmod{2^{2r+2}}. \quad (1)
\end{aligned}$$

Kohdassa $*$ käytetään apuna lausetta 3.8.

Eli

$$t2^{s-1} = (n-1)/2 \equiv 2^r \sum_{i=1}^{m} a_i d_i \pmod{2^{2r+1}}. \quad (2)$$

Kongruenssista seuraa, että

$$t2^{s-1-r} \equiv \sum_{i=1}^{m} a_i d_i \pmod{2^{r+1}}.$$

ja

$$b^{(n-1)/2} = (b^{2^r t})^{2^{s-1-r}} \equiv (-1)^{2^{s-1-r}} = (-1)^{\sum_{i=1}^{m} a_i d_i} \pmod{n}. \quad (3.2)$$

Toisaalta yhtälön (3.1) perusteella tiedetään, että

$$\left(\frac{b}{n}\right) = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{a_i} = \prod_{i=1}^{m} ((-1)^{d_i})^{a_i} = \prod_{i=1}^{m} (-1)^{a_i d_i} = (-1)^{\sum_{i=1}^{m} a_i d_i}.$$

Yhdistämällä yhtälöt (3.1) ja (3.2), nähdään, että

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Nyt siis n on Eulerin pseudoalkuluku kannan b suhteen. □

Huomautus 3.1. Edellisen lauseen todistus on tehty Rosenin kirjan Elementary Number Theory and Its Applications pohjalta, mutta kirjan todistus sisältää virheitä kohdissa (1) ja (2).

Vaikka jokainen vahva pseudoalkuluku kannan b suhteen on Eulerin pseudoalkuluku saman kannan suhteen, pitää huomata, että jokainen Eulerin pseudoalkuluku kannan b suhteen ei ole vahva pseudoalkuluku saman kannan suhteen. Seuraavaksi esitetään esimerkki tästä.

Esimerkki 3.10. Aiemmin esitettiin, että 561 on Eulerin pseudoalkuluku kannan 2 suhteen. Kuitenkaan 561 ei ole vahva pseudoalkuluku kannan 2 suhteen, koska

$$2^{(561-1)/2} = 2^{280} \equiv 1 \pmod{561},$$

vaikka

$$2^{(561-1)/2^2} = 2^{70} \equiv 166 \not\equiv \pm 1 \pmod{561}.$$

On kuitenkin mahdollista lisätä ehtoja, jotta jokaisesta Eulerin pseudoalkuluvusta, joka täyttää kyseiset kriteerit, kannan b suhteen, saadaan vahva pseudoalkuluku. Seuraavaksi esitetään kyseiset ehdot.

Lause 3.10. *Jos $n \equiv 3$ (mod 4) ja n on Eulerin pseudoalkuluku kannan b suhteen, niin n on vahva pseudoalkuluku kannan b suhteen.*

Todistus. (Vrt. [8, s. 457].) Kongruenssin $n \equiv 3 \pmod 4$ perusteella tiedetään, että $n - 1 = 2 \cdot t$, missä $t = (n-1)/2$ on pariton. Tämä pätee, koska

$$\begin{aligned} n - 3 &= 4k \\ n - 1 &= 4k + 2 \\ &= 2(2k + 1) \\ &= 2t, \end{aligned}$$

missä t on pariton kokonaisluku. Koska n on Eulerin pseudoalkuluku kannan b suhteen, seuraa siitä, että

$$b^t = b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Koska $\left(\frac{b}{n}\right) = \pm 1$, tiedetään, että $b^t \equiv 1 \pmod n$ tai $b^t \equiv -1 \pmod n$.

Siis yhden vahvan pseudoalkuluvun määritelmässä olevista kongruensseista tulee pitää paikkansa, joten n on vahva pseudoalkuluku kannan b suhteen. □

Lause 3.11. *Jos n on Eulerin pseudoalkuluku kannan b suhteen ja $\left(\frac{b}{n}\right) = -1$, niin n on vahva pseudoalkuluku kannan b suhteen.*

Todistus. (Ks. [8, s. 457].) Merkitään $n - 1 = 2^s t$, missä t on pariton. Koska n on Eulerin pseudoalkuluku kannan b suhteen, niin n on pariton ja siten $s \geq 1$, ja täten saadaan

$$b^{2^{s-1}t} = b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Mutta koska $\left(\frac{b}{n}\right) = -1$, huomataan, että

$$b^{t2^{s-1}} \equiv -1 \pmod{n}.$$

Tämä on yksi vahvan pseudoalkuluvun määritelmän kongruensseista. Koska n on yhdistetty luku, on se vahva pseudoalkuluku kannan b suhteen. □

3.6 Lucas'n pseudoalkuluvut

Määritelmä 3.6. Lucas'n jonot parametrein P ja Q ovat $\{u_n\}$ ja $\{v_n\}$, jotka määritellään seuraavasti:

$$u_0 = 0, u_1 = 1 \text{ ja } u_n = Pu_{n-1} - Qu_{n-2},$$
$$v_0 = 2, v_1 = P \text{ ja } v_n = Pv_{n-1} - Qv_{n-2},$$

kun $n \geq 2$.

Joskus jonoja merkitään myös $u_n = u_n(P, Q)$ ja $v_n = v_n(P, Q)$, jos halutaan korostaa riippuvuutta parametreistä P ja Q. Olkoon $x^2 - Px + Q$ Lucas'n jonoon liittyvä karakteristinen polynomi, olkoon $D = P^2 - 4Q$ sen diskriminantti ja olkoot α ja β kaksi karakteristisen polynomin nollakohtaa.

Fibonaccin luvut saadaan jonona u_n, jos $P = 1$ ja $Q = -1$. Jos u_n määritellään Fibonaccin luvuiksi, niin lukuja $v_n = v_n(1, -1)$ kutsutaan Lucasin luvuiksi. Karakteristinen polynomi on tässä tapauksessa $x^2 - x - 1$, jonka diskriminantti on $D = 5$ ja nollakohdat ovat $\alpha, \beta = (1 \pm \sqrt{5})/2$.

Oletetaan, että parametrit P ja Q ovat kokonaislukuja, minkä seurauksena myös kaikki u_n:t ja v_n:t ovat kokonaislukuja. Yleensä oletetaan myös, että $D = P^2 - 4Q$ ei ole neliö, jolloin pätee, että $D \neq 0$, joten $\alpha \neq \beta$.

Yhtälöstä $(x - \alpha)(x - \beta) = x^2 - x(\alpha + \beta) + \alpha\beta = x^2 - Px + Q$ nähdään, että $\alpha + \beta = P$ ja $\alpha\beta = Q$. Nyt jos $\alpha = (P + \sqrt{D})/2$ ja $\beta = (P - \sqrt{D})/2$, niin $\alpha - \beta = \sqrt{D}$. Todistamme lauseessa 3.12, että

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{D}} \text{ ja } v_n = \alpha^n + \beta^n,$$

kun $n \geq 0$. Näitä yhtälöitä kutsutaan Binetin yhtälöiksi.

Huomautus 3.2. Seuraavaa todistusta ei löydy lähteenä käytetystä kirjasta.

Lause 3.12. *Olkoon $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$ ja $D = 5$. Yhtälöt*

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{D}} \textit{ ja } v_n = \alpha^n + \beta^n,$$

pätevät, kun $n \geq 0$.

Todistus. Nyt koska Lucasin jonoon liittyvä karakteristinen polynomi on $x^2 - x - 1$ ja α ja β ovat sen nollakohtia, niin seuraavat yhtälöt pätevät:

$$\alpha^{k+1} = \alpha^k + \alpha^{k-1},$$
$$\beta^{k+1} = \beta^k + \beta^{k-1},$$

koska

$$0 = (\alpha^2 - \alpha - 1)\alpha^{k-1} = \alpha^{k+1} - \alpha^k - \alpha^{k-1}$$
$$\alpha^{k+1} = \alpha^k - \alpha^{k-1}$$

sekä

$$0 = (\beta^2 - \beta - 1)\beta^{k-1} = \beta^{k+1} - \beta^k - \beta^{k-1}$$
$$\beta^{k+1} = \beta^k - \beta^{k-1},$$

kun $k \geq 2$.

Todistetaan lause induktiolla.

1. Olkoon $n = 1$. Nyt siis

$$\frac{\alpha^1 - \beta^1}{\sqrt{5}} = \frac{1 + \sqrt{5} - 1 + \sqrt{5}}{2\sqrt{5}} = 1 = u_1$$

ja

$$\alpha^1 + \beta^1 = \frac{1 + \sqrt{5}}{2} + \frac{1 - \sqrt{5}}{2} = 1 = v_1.$$

2. Oletetaan, että yhtälöt pätevät, kun $n = k \geq 1$.

3. Olkoon $n = k + 1$. Nyt siis

$$\begin{aligned} u_{k+1} = u_{k-1} + u_k &= \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}} - \frac{\alpha^k - \beta^k}{\sqrt{5}} \\ &= \frac{\alpha^{k-1} - \alpha^k - (\beta^{k-1} - \beta^k)}{\sqrt{5}} \\ &= \frac{\alpha^{k+1} - \beta^{k+1}}{\sqrt{5}} \end{aligned}$$

sekä

$$\begin{aligned} v_{k+1} = v_{k-1} + v_k &= \alpha^{k-1} + \beta^{k-1} + \alpha^k + \beta^k \\ &= \alpha^{k-1} + \alpha^k + \beta^{k-1} + \beta^k \\ &= \alpha^{k+1} + \beta^{k+1}. \end{aligned}$$

□

On olemassa luonnollinen tapa laskea Lucasin lukuja käyttämällä $2x2$-matriiseja. Merkitään

$$L = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix} \text{ ja kun } n \geq 0, A_n = \begin{bmatrix} u_{n+1} & v_{n+1} \\ u_n & v_n \end{bmatrix}.$$

Silloin

$$A_0 = \begin{bmatrix} 1 & P \\ 0 & 2 \end{bmatrix}.$$

Osoitetaan seuraavaksi yksinkertaisella induktiolla, että $A_n = L^n A_0$, kun $n \geq 0$, missä L^0 tarkoittaa identiteettimatriisia.

Lause 3.13. *Olkoon*

$$L = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix} \text{ ja kun } n \geq 0, A_n = \begin{bmatrix} u_{n+1} & v_{n+1} \\ u_n & v_n \end{bmatrix}.$$

Kun $n \geq 0$, pätee

$$A_n = L^n A_0.$$

Todistus. Todistetaan väite induktiolla.

1. Olkoon $n = 0$. Nyt $A_0 = \begin{bmatrix} 1 & P \\ 0 & 2 \end{bmatrix}$ ja $L^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, joten siis $A_0 = L^0 A_0 = A_0$.
2. Oletetaan, että seuraava yhtälö pätee; $A_n = L^n A_0$.
3. Nyt

$$A_{n+1} = \begin{bmatrix} u_{n+2} & v_{n+2} \\ u_{n+1} & v_{n+1} \end{bmatrix}.$$

Tavoitteena on osoittaa, että $A_{n+1} = L^{n+1} A_0$. Yhtälö voidaan muokata seuraavaan muotoon; $A_{n+1} = LL^n A_0$. Tiedetään, että $A_n = L^n A_0$, joten $A_{n+1} = LA_n$. Siis

$$\begin{aligned} A_{n+1} = LA_n &= \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_{n+1} & v_{n+1} \\ u_n & v_n \end{bmatrix} \\ &= \begin{bmatrix} Pu_{n+1} - Qu_n & Pv_{n+1} - Qv_n \\ u_{n+1} & v_{n+1} \end{bmatrix} \\ &= \begin{bmatrix} u_{n+2} & v_{n+2} \\ u_{n+1} & v_{n+1} \end{bmatrix} = A_{n+1}. \end{aligned}$$

□

Huomautus 3.3. Yllä esitettyä induktiotodistusta ei ole lähteenä käytetyssä kirjassa.

Lause 3.14. *Olkoon $n \geq 0$. Silloin pätee*

$$2^{n-1} u_n = \sum_{\substack{i=0 \\ i \text{ pariton}}}^{n} \binom{n}{i} P^{n-i} D^{(i-1)/2},$$

$$2^{n-1} v_n = \sum_{\substack{i=0 \\ i \text{ parillinen}}}^{n} \binom{n}{i} P^{n-i} D^{i/2}.$$

Todistus. (Vrt. [9, s. 162].)Aloitetaan jonon u_n kaavasta ja käsitellään karakteristisen polynomin kahta nollakohtaa.

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{(P + \sqrt{D})^n - (P - \sqrt{D})^n}{2^n \sqrt{D}}.$$

Käytetään binomikaavaa ja saadaan

$$u_n = \frac{\sum_{i=0}^{n} \binom{n}{i} P^{n-i} (\sqrt{D})^i - \sum_{i=0}^{n} \binom{n}{i} P^{n-i} (-\sqrt{D})^i}{2^n \sqrt{D}}$$

$$2^n u_n = \frac{1}{\sqrt{D}} \sum_{i=0}^{n} \binom{n}{i} P^{n-i} ((\sqrt{D})^i - (-\sqrt{D})^i).$$

Kun i on parillinen, erotuksen $(\sqrt{D})^i - (-\sqrt{D})^i$ jälkimmäisen termin miinusmerkki häviää. Jos taas i on pariton, miinukset kumoavat toisensa. Siis

$$2^n u_n = \frac{2}{\sqrt{D}} \sum_{\substack{i=0 \\ i \text{ pariton}}}^{n} \binom{n}{i} P^{n-i} (\sqrt{D})^i.$$

Lauseen ensimmäinen yhtälö saadaan jakamalla ylläoleva yhtälö luvulla 2 ja supistamalla yhdet $\sqrt{D}$:t.

Seuraavaksi otetaan käsittelyyn kaava

$$v_n = \alpha^n + \beta^n = \frac{(P + \sqrt{D})^n + (P - \sqrt{D})^n}{2^n}.$$

Käyttämällä binomikaavaa saadaan

$$v_n = \frac{\sum_{i=0}^{n} \binom{n}{i} P^{n-i} (\sqrt{D})^i + \sum_{i=0}^{n} \binom{n}{i} P^{n-i} (-\sqrt{D})^i}{2^n}$$

$$2^n v_n = \sum_{i=0}^{n} \binom{n}{i} P^{n-i} ((\sqrt{D})^i + (-\sqrt{D})^i).$$

Nyt erotuksen $(\sqrt{D})^i + (-\sqrt{D})^i$ jälkimmäisen termin miinusmerkki häviää, joten

$$2^n v_n = 2 \sum_{\substack{i=0 \\ i \text{ parillinen}}}^{n} \binom{n}{i} P^{n-i} (\sqrt{D})^i.$$

Siis

$$2^{n-1} v_n = \sum_{\substack{i=0 \\ i \text{ parillinen}}}^{n} \binom{n}{i} P^{n-i} (\sqrt{D})^i.$$

□

Lause 3.15. *Jos n on alkuluku, u_i on i:s Fibonaccin luku ja $\left(\frac{n}{5}\right)$ on vastaava Legendren symboli, niin n jakaa luvun $u_{n-\left(\frac{n}{5}\right)}$.*

Seuraava lause yleistää ylläolevan lauseen ja todistaa myös sen.

Lause 3.16. *Jos p on pariton alkuluku, joka ei jaa lukua PQ, niin*

$$u_{p-\left(\frac{D}{p}\right)} \equiv 0 \pmod{p},$$

$$u_p \equiv \left(\frac{D}{p}\right) \pmod{p} \text{ ja}$$

$$v_p \equiv v_1 = P \pmod{p}.$$

Jos myös $\operatorname{syt}(p, D) = 1$*, niin*

$$v_{p-\left(\frac{D}{p}\right)} \equiv 2Q^{(1-\left(\frac{D}{p}\right))/2} \pmod{p}.$$

Todistus. (Vrt. [9, s. 162-163].)Olkoon $n = p$ luvun u_n kaavassa

$$2^{n-1}u_n = \sum_{\substack{i=0 \\ i \text{ pariton}}}^{n} \binom{n}{i} P^{n-i} D^{(i-1)/2}$$

lauseessa 3.14. Huomataan, että koska p on alkuluku, se jakaa kaikki binomikertoimet $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, kun $1 \leq i \leq n-1$. Ainoa termi summassa on se, jossa $i = p$, muut termit ovat $\equiv 0 \pmod{p}$. Myöskin pätee $2^{p-1} \equiv 1 \pmod{p}$ Fermat'n pienen lauseen mukaan. Huomataan, että koska

$$2^{p-1}u_p = \sum_{i=0}^{p} \binom{p}{i} P^{p-i} D^{(i-1)/2},$$

niin

$$u_p \equiv D^{(p-1)/2} \equiv \left(\frac{D}{p}\right) \pmod{p}$$

Eulerin kriteerin mukaan. Tämä todistaa toisen kaavan.

Ensimmäisen yhtälön todistamiseksi oletetaan, että $n = p + 1$ luvun u_n kaavassa

$$2^{n-1}u_n = \sum_{\substack{i=0 \\ i \text{ pariton}}}^{n} \binom{n}{i} P^{n-i} D^{(i-1)/2}$$

lauseessa 3.14. Koska p on alkuluku, se jakaa kaikki binomikertoimet $\binom{p+1}{i}$, kun $2 \leq i \leq p-1$. Ainoat parittomat indeksit i, jotka eivät ole tässä intervallissa, ovat $i = 1$ ja $i = p$, joten summa kutistuu kahteen termiin. Saadaan $2^p \equiv 2 \pmod{p}$ Fermat'n pienen lauseen mukaan. Huomataan nyt, että

$$2u_{p+1} \equiv (p+1)P^p D^0 + (p+1)P^1 D^{(p-1)/2} \equiv P(1 + \left(\frac{D}{p}\right)) \pmod{p},$$

missä käytetään kongruensssia $p \equiv 0 \pmod{p}$, kongruenssia $P^p \equiv P \pmod{p}$ Fermat'n pienen lauseen mukaan sekä Eulerin kriteeriä. Jos $\left(\frac{D}{p}\right) = -1$, nähdään heti, että p jakaa luvun $u_{p+1} = u_{p-\left(\frac{D}{p}\right)}$. Jos taas $\left(\frac{D}{p}\right) = 1$, saadaan $2u_{p+1} \equiv 2P \pmod{p}$, joten $u_{p+1} \equiv P \pmod{p}$. Toisen kaavan mukaan $u_p \equiv \left(\frac{D}{p}\right) = 1 \pmod{p}$. Sijoittamalla nämä rekursiokaavaan $u_{p+1} = Pu_p - Qu_{p-1}$, saadaan $P \equiv P(1) - Qu_{p-1} \pmod{p}$. Tästä seuraa, että $Qu_{p-1} \equiv 0 \pmod{p}$. Koska $\text{syt}(p, Q) = 1$, voidaan kongruenssi jakaa luvulla Q. Silloin huomataan, että p jakaa luvun $u_{p-1} = u_{p-\left(\frac{D}{p}\right)}$.

Olkoon $n = p$ luvun v_n kaavassa

$$2^{n-1}v_n = \sum_{\substack{i=0 \\ i \text{ parillinen}}}^{n} \binom{n}{i} P^{n-i} D^{i/2}$$

lauseessa 3.16. Nyt taas koska p on alkuluku, se jakaa kaikki binomikertoimet $\binom{p}{i}$, kun $1 \leq i \leq n-1$. Samoin pätee taas kongruenssi $2^{p-1} \equiv 1 \pmod{p}$. Summaan jää ainoastaan termi, jossa $i = 0$. Siis

$$v_p \equiv P = v_1 \pmod{p}.$$

Siis kolmas yhtälö pätee.

Oletetaan seuraavaksi, että $n = p + 1$ luvun v_n kaavassa

$$2^{n-1} v_n = \sum_{\substack{i=0 \\ i \text{ parillinen}}}^{n} \binom{n}{i} P^{n-i} D^{i/2}$$

lauseessa 3.14. Luku p jakaa taas kaikki binomikertoimet $\binom{p+1}{i}$, kun $2 \leq i \leq p-1$. Muut parilliset indeksit ovat $i = 0$ ja $i = p + 1$, joten summaan jää kaksi termiä. Fermat'n pienen lauseen mukaan $2^p \equiv 2 \pmod{p}$. Nyt siis

$$2^{n-1} v_n \equiv 2v_{p+1} \equiv 1 \cdot P^{p+1} D^{0/2} + 1 \cdot P^0 D^{(p+1)/2} \equiv P^{p+1} + D^{(p+1)/2} \pmod{p}.$$

Käytetään Fermat'n lausetta ja Eulerin kriteeriä kongruenssiin ja saadaan

$$\begin{aligned} 2v_{p+1} &\equiv P^2 + (D^{p-1} \cdot D^2)^{1/2} \pmod{p} \\ &\equiv P^2 + D^{(p-1)/2} \cdot D \pmod{p} \\ &\equiv P^2 + \left(\frac{D}{p}\right) \cdot D \pmod{p}. \end{aligned}$$

Oletetaan seuraavaksi, että $\left(\frac{D}{p}\right) = 1$. Nyt siis

$$2v_{p+1} \equiv P^2 + D \pmod{p}.$$

Koska $P^2 = D + 4Q$ on karakteristisen polynomin diskriminantti, niin

$$2v_{p+1} \equiv D + 4Q + D = 2D + 4Q \pmod{p}.$$

Koska Lucasin jonon alkiot määritellään kaavalla $v_{p+1} = Pv_p - Qv_{p-1}$, sijoitetaan se kongruenssiin, jolloin saadaan

$$\begin{aligned} 2(Pv_p - Qv_{p-1}) &\equiv D + 4Q + D = 2D + 4Q \pmod{p} \\ 2Pv_p - 2Qv_{p-1} &\equiv 2D + 4Q \pmod{p}. \end{aligned}$$

Käytetään seuraavaksi äsken osoitettua kongruenssia $v_p \equiv v_1 = P \pmod{p}$, ja saadaan

$$\begin{aligned} 2P^2 - 2Qv_{p-1} &\equiv 2D + 4Q \pmod{p} \\ 2(D + 4Q) - 2Qv_{p-1} &\equiv 2D + 4Q \pmod{p}. \end{aligned}$$

Nyt molemmilta puolilta voidaan vähentää $2D$ ja $4Q$, jolloin saadaan

$$4Q - 2Qv_{p-1} \equiv 0 \pmod{p}.$$

Koska $\text{syt}(2Q, p) = 1$, voidaan kongruenssi jakaa luvulla $2Q$, joten

$$\begin{aligned} 2 - v_{p-1} &\equiv 0 \pmod{p} \\ v_{p-1} &\equiv 2 \pmod{p}. \end{aligned}$$

Oletetaan sitten, että $\left(\frac{D}{p}\right) = -1$. Siis

$$2v_{p+1} \equiv P^2 - D \pmod{p}.$$

Karakteristisen polynomin diskriminantti on $D = P^2 - 4Q$, ja hieman yhtälöä muokkaamalla saadaan $4Q = P^2 - D$. Sijoitetaan saatu yhtälö kongruenssiin, joten

$$2v_{p+1} \equiv 4Q \pmod{p}.$$

Nyt jakamalla kongruenssi luvulla 2 saadaan haluttu kongruenssi

$$v_{p+1} \equiv 2Q \pmod{p}.$$

□

Olkoon I 2×2-identiteettimatriisi.

Lause 3.17. *Jos A on nxn-kokoinen kokonaislukumatriisi ja m on positiivinen kokonaisluku siten, että* $\text{syt}(\det A, m) = 1$*, matriisi* $\overline{A} = \overline{\det A}(\text{adj}\, A)$ *on matriisin A käänteismatriisi modulo m, missä* $\overline{\det A}$ *on determinantin $\det A$ käänteisluku modulo m.*

Todistus. (Ks. [8, s. 183]). Olkoon $\text{syt}(\det A, m) = 1$, joten tiedetään suoraan, että $\det A \neq 0$. Siis koska $\det A \neq 0$, saadaan, että

$$A(\text{adj}\, A) = (\det A)I.$$

Koska $\text{syt}(\det A, m) = 1$, on olemassa determinantin käänteisluku $\overline{\det A}$ modulo m. Siis

$$A\,\overline{\det A}(\text{adj}\, A) \equiv A\,(\text{adj}\, A)\overline{\det A} \equiv \det A\,\overline{\det A}\, I \equiv I \pmod{m},$$

ja

$$\overline{\det A}(\text{adj}\, A)A \equiv \overline{\det A}((\text{adj}\, A)A) \equiv \overline{\det A}(\det A)I \equiv I \pmod{m}.$$

Siis $\overline{A} = \overline{\det A}(\text{adj}\, A)$ on matriisin A käänteismatriisi modulo m. □

Lause 3.18. *Olkoon* $L = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix}$ *matriisi, jota käytetään Lucasin lukujen laskemiseen parametreina P ja Q. Olkoon $D = P^2 - 4Q$. Olkoon p alkuluku, joka ei jaa lukua $2PQD$. Jos* $\left(\frac{D}{p}\right) = 1$*, niin* $L^{p-1} \equiv I \pmod{p}$*. Joka tapauksessa* $L^{p^2-1} \equiv I \pmod{p}$*.*

Todistus. (Ks. [9, s. 163-164].) Olkoon $\left(\frac{D}{p}\right) = 1$. Lauseen 3.16 mukaan

$$A_{p-1} = \begin{bmatrix} u_p & v_p \\ u_{p-1} & v_{p-1} \end{bmatrix} \equiv \begin{bmatrix} 1 & P \\ 0 & 2 \end{bmatrix} = A_0 \pmod{p}.$$

Mutta myöskin pätee $A_{p-1} = L^{p-1}A_0$ lauseen 3.13 mukaan. Koska matriisin A_0 determinantti on 2, se on kääntyvä modulo p. Siis $L^{p-1} \equiv I \pmod{p}$, koska $A_0 \equiv L^{p-1}A_0 \pmod{p}$. Nyt saadaan

$$L^{p^2-1} = (L^{p-1})^{p+1} \equiv I^{p+1} = I \pmod{p}.$$

Oletetaan seuraavaksi, että $\left(\frac{D}{p}\right) = -1$. Lauseen 3.16 mukaan

$$A_p = L^p A_0 = \begin{bmatrix} u_{p+1} & v_{p+1} \\ u_p & v_p \end{bmatrix} \equiv \begin{bmatrix} 0 & 2Q \\ -1 & P \end{bmatrix} \pmod{p}.$$

Koska A_0 on kääntyvä modulo p, ja lauseen 3.17 mukaan sen käänteismatriisi $\overline{A_0} \equiv \frac{1}{2}\begin{bmatrix} 2 & -P \\ 0 & 1 \end{bmatrix} \pmod{p}$. Siis $L^p \equiv A_p\overline{A_0} \equiv \begin{bmatrix} 0 & 2Q \\ -1 & P \end{bmatrix}\begin{bmatrix} 1 & -P/2 \\ 0 & 1/2 \end{bmatrix} \equiv \begin{bmatrix} 0 & Q \\ -1 & P \end{bmatrix} \pmod{p}$ ja $L^{p+1} = LL^p \equiv \begin{bmatrix} Q & 0 \\ 0 & Q \end{bmatrix} = QI \pmod{p}$. Nyt

$$L^{p^2-1} = (L^{p+1})^{p-1} \equiv Q^{p-1}I \equiv I \pmod{p}$$

Fermat'n pienen lauseen mukaan. □

Määritelmä 3.7. Lucasin todennäköinen alkuluku parametrein P ja Q on kokonaisluku $n(> 1)$, joka toteuttaa ehdot $\text{syt}(n, 2PQD) = 1$ ja $u_{n-\left(\frac{D}{n}\right)} \equiv 0 \pmod{n}$, missä $D = P^2 - 4Q$.

Lucasin pseudoalkuluku parametrein P ja Q on yhdistetty Lucasin todennäköinen alkuluku samoilla parametreilla.

4 Alkulukutestauksesta

On todella kallista ja aikaavievää todistaa, että annettu positiivinen kokonaisluku on alkuluku. On kuitenkin olemassa tehokkaita algoritmeja, jotka osoittavat luvun olevan alkuluku korkealla todennäköisyydellä. Tälläisiä algoritmeja kutsutaan alkulukutesteiksi.

4.1 Fermat'n alkulukutesti

Ensimmäinen esimerkki alkulukutesteistä on Fermat'n alkulukutesti. Se pohjautuu Fermat'n pieneen lauseeseen seuraavassa muodossa:

Lause 4.1. *Jos n on alkuluku, $a^{n-1} \equiv 1 \pmod{n}$ kaikilla luvuilla $a \in \mathbb{Z}$, kun* $\text{syt}(a, n) = 1$.

Todistus. (Ks. Lause 2.9). □

Tätä lausetta voidaan käyttää määrittämään, onko positiivinen kokonaisluku yhdistetty luku. Valitaan positiivinen kokonaisluku $a \in \{1, 2, ..., n-1\}$. Lasketaan seuraavaksi $y \equiv a^{n-1} \pmod{n}$. Jos $y \neq 1$, niin n on yhdistetty luku Fermat'n pienen lauseen perusteella. Jos taas $y = 1$, ei tiedetä, onko n yhdistetty luku vai ei, kuten seuraava esimerkki osoittaa.

Esimerkki 4.1. (Ks. [1, s. 130].) Olkoon $n = 341 = 11 \cdot 31$. Nyt saadaan

$$2^{340} \equiv 1 \pmod{341},$$

vaikka n on yhdistetty luku. Joten jos käytetään Fermat'n alkulukutestiä luvuin $n = 341$ ja $a = 2$, saadaan $y = 1$, mikä ei todista mitään. Toisaalta saadaan myös

$$3^{340} \equiv 56 \pmod{341}.$$

Siis jos käytetään Fermat'n alkulukutestiä luvuin $n = 341$ ja $a = 3$, niin n on osoitettu yhditetyksi luvuksi.

Vaikka Fermat'n alkulukutesti osoittaa, että n on yhdistetty luku, se ei löydä silti luvun n tekijöitä. Se osoittaa ainoastaan, että luvulla n ei ole sellaista ominaisuutta, joka kaikilla alkuluvuilla on. Siksi Fermat'n alkulukutestiä ei voi käyttää tekijäalgoritmina.

4.2 Pepinin alkulukutesti

Muotoa $F_n = 2^{2^n} + 1$ olevia kokonaislukuja kutsutaan Fermat'n luvuiksi. Fermat väitti, että kaikki näin saatavat kokonaisluvut olisivat alkulukuja. F_1, F_2, F_3, F_4 ovatkin alkulukuja, mutta jo $F_5 = 2^{2^5} + 1$ on yhdistetty luku.

Esimerkki 4.2. (Ks. [8, s. 131-132].) Fermat'n luku $F_5 = 2^{2^5} + 1$ on jaollinen luvulla 641. Nimittäin

$$\begin{aligned} 2^{2^5} + 1 &= 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = (641 - 5^4) \cdot 2^{28} + 1 \\ &= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641 \cdot (2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4). \end{aligned}$$

Siis $641 \mid F_5$.

Lause 4.2 (Pepinin testi)**.** *Fermat'n luku $F_m = 2^{2^m} + 1$ on alkuluku, jos ja vain jos*

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

Todistus. (Vrt. [8, s. 438-439].) Näytetään ensin, että F_m on alkuluku, jos lauseen kongruenssi pätee. Oletetaan siis, että

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

Korottamalla molemmat puolet toiseen potenssiin saadaan

$$3^{(F_m-1)} \equiv 1 \pmod{F_m}.$$

Jos p on alkuluku, joka jakaa luvun F_m, niin saadaan

$$3^{(F_m-1)} \equiv 1 \pmod{p},$$

eli siis lauseen 2.13 mukaan

$$\operatorname{ord}_p 3 \mid (F_m - 1) = 2^{2^m}.$$

Näin ollen kertaluvun $\operatorname{ord}_p 3$ tulee olla luvun 2 potenssi. Kuitenkin

$$\operatorname{ord}_p 3 \nmid 2^{2^m-1} = (F_m - 1)/2,$$

koska $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$. Nyt ainoa mahdollisuus on, että $\operatorname{ord}_p 3 = 2^{2^m} = F_m - 1$. Koska Fermat'n pienen lauseen ja kertaluvun määritelmän mukaan $\operatorname{ord}_p 3 \leq p - 1$, niin $F_m - 1 \leq p - 1$ eli $F_m \leq p$, ja koska $p \mid F_m$, niin $p \leq F_m$. Nyt nähdään, että $p = F_m$, joten F_m on alkuluku.

Oletetaan seuraavaksi, että $F_m = 2^{2^m} + 1$ on alkuluku. Nyt jos F_m on alkuluku, kun $m \geq 1$, resiprookkilause kertoo, että

$$\left(\frac{3}{F_m}\right) = \left(\frac{F_m}{3}\right) = \left(\frac{2}{3}\right) = -1, \tag{4.1}$$

koska $F_m \equiv 1 \pmod 4$ ja $F_m \equiv 2 \pmod 3$.

Käyttämällä Eulerin kriteeriä tiedetään, että

$$\left(\frac{3}{F_m}\right) \equiv 3^{(F_m-1)/2} \pmod{F_m}. \tag{4.2}$$

Käyttämällä yhtälöitä (4.1) ja (4.2) saadaan

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

Tämä täydentää todistuksen. □

Esimerkki 4.3. (Ks. [8, s. 439].) Olkoon $m = 2$. Nyt $F_2 = 2^{2^2} + 1 = 17$ ja

$$3^{(F_2-1)/2} = 3^8 \equiv -1 \pmod{17}.$$

Pepinin testillä nähdään, että $F_2 = 17$ on alkuluku.

Olkoon $m = 5$. Nyt $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,297$. Lasketaan

$$3^{(F_5-1)/2} = 3^{2^{31}} = 3^{2\,147\,483\,648} \equiv 10\,324\,303 \not\equiv -1 \pmod{4\,294\,967\,297}.$$

Pepinin testin perusteella nähdään, että F_5 on yhdistetty luku.

4.3 Lucas'n ja Lehmerin alkulukutesti

Luvun todistamisen alkuluvuksi tulisi olla nopeaa ja helppoa todistaa. Tämän vuoksi luvun jaollisuuden testaaminen pelkästään jakamalla kyseistä lukua mahdollisilla tekijöillä ei toimi, koska ensinnäkin se voi kestää todella kauan ja toiseksi, jotta voitaisiin todistaa sen paikkansapitävyys, täytyisi laskut tehdä kokonaan uudestaan.

Seuraavan alkulukutestin idea on käyttää sitä faktaa, että $\phi(n) = n - 1$, jos ja vain jos n on alkuluku. Tietenkään ei ole olemassa mitään tiedettyä keinoa laskea lukua $\phi(n)$ ilman luvun n tekijöihinjakoa, joten on keksittävä toinen keino näyttää, että $\phi(n) = n - 1$. Jos löydetään kokonaisluku a, jonka kertaluku modulo n on $n - 1$, niin $n - 1 \mid \phi(n)$, koska $\mathrm{ord}_n a \mid \phi(n)$. Toisaalta $\phi(n) \leq n - 1$, joten $\phi(n) = n - 1$. Esitettävän alkulukutestin kehitti Lucas vuonna 1876 ja se julkaistiin ensimmäisen kerran vuonna 1927 D. H. Lehmerin toimesta.

Lause 4.3 (Lucas-Lehmer alkulukutesti)**.** *Oletetaan, että on olemassa kokonaisluku a siten, että $a^{n-1} \equiv 1 \pmod{n}$, mutta jokaiselle alkuluvulle q, joka jakaa luvun $n-1$, pätee $a^{(n-1)/q} \not\equiv 1 \pmod{n}$, niin n on alkuluku.*

Todistus. (Vrt. [5, s. 186].) Todistuksen tavoitteena on näyttää, että $\mathrm{ord}_n a = n - 1$.

Kongruenssin $a^{n-1} \equiv 1 \pmod{n}$ perusteella tiedetään, koska a ja n ovat keskenään jaottomia, että $\mathrm{ord}_n a \mid n-1$. Siis $n-1 = \mathrm{ord}_n a \cdot k$ jollakin luvulla k. Seuraavaksi halutaan osoittaa, että $k = 1$. Tehdään vastaoletus, että $k > 1$. Nyt jokin alkuluku q jakaa luvun k, joten on olemassa luku l siten, että $k = lq$. Silloin $q \mid n - 1$, joten voidaan kirjoittaa

$$a^{(n-1)/q} \equiv a^{\mathrm{ord}_n a \cdot k/q} \equiv a^{\mathrm{ord}_n a \cdot l} \equiv 1 \pmod{n}.$$

Tämä ei voi pitää paikkaansa lauseen oletusten takia, joten $k = 1$ ja $\mathrm{ord}_n a = n - 1$. Koska $\mathrm{ord}_n a \mid \phi(n)$ (lause 2.13), on oltava $\phi(n) \geq n - 1$, mutta $\phi(n) \leq n - 1$, joten $\phi(n) = n - 1$ ja n on alkuluku. □

Esimerkki 4.4. (Ks. [5, s.187].) Olkoon $n = 29$. Nyt $n - 1 = 28 = 2^2 7$. Olkoon $a = 2$. Lasketaan Lucas-Lehmer alkulukutestin määräämät kongruenssit:

$$
\begin{aligned}
2^{28} &\equiv 1 \pmod{29} \\
2^{28/2} &\equiv 28 \not\equiv 1 \pmod{29} \\
2^{28/7} &\equiv 16 \not\equiv 1 \pmod{29}.
\end{aligned}
$$

Lucas-Lehmer alkulukutestin (lause 4.3) ehdot täyttyvät, joten 29 on alkuluku.

Esimerkki 4.5. (Ks. [5, s. 187].) Olkoon $n = 2071723$. Saadaan, että

$$n - 1 = 2 \cdot 3 \cdot 17 \cdot 19 \cdot 1069$$

ja merkitään $a = 2$, niin Lucas-Lehmer alkulukutestin kongruensseiksi saadaan

$$
\begin{aligned}
2^{n-1} &\equiv 1 \pmod{n} \\
2^{(n-1)/2} &\equiv -1 \pmod{n} \\
2^{(n-1)/3} &\equiv 321129 \pmod{n} \\
2^{(n-1)/17} &\equiv 100000 \pmod{n} \\
2^{(n-1)/19} &\equiv 71064 \pmod{n} \\
2^{(n-1)/1069} &\equiv 1573595 \pmod{n}.
\end{aligned}
$$

Kaikki Lucas-Lehmer alkulukutestin ehdot täyttyvät, joten n on alkuluku.

On tärkeää todeta ensin, että kongruenssi $a^{n-1} \equiv 1 \pmod{n}$ pätee. Ilman tätä ehtoa todistuksen loppuosa ei voi toimia.

Tämä kokonaisluku a, joka toteuttaa edellä mainitun ehdon, on primitiivinen juuri. Useimmiten primitiivinen juuri löydetään helposti käymällä läpi pieniä positiivisia kokonaislukuja $2, 3, 4, \ldots$ Kuitenkin joissakin tapauksissa pienin primitiivinen juuri voi olla hyvinkin iso, joten sen löytämiseen voi mennä paljon aikaa. Seuraava parannus ehtoihin osoittaa, että ei tarvitse löytää privitiivistä juurta todistaakseen, että $\phi(n) = n - 1$.

Jos kokonaisluku a ei toteuta kongruenssiehtoa Lucas-Lehmer alkulukutestissä, on olemassa q siten, että $a^{(n-1)/q} \equiv 1 \pmod{n}$. On mahdollista, että monille muille alkuluvuille q' pätee $a^{(n-1)/q'} \not\equiv 1 \pmod{n}$. Käytetään mielummin tätä ehtoa kuin yritettäisiin etsiä kokonaan uusi arvo a:lle. Seuraava lause osoittaa, miten tätä tietoa voidaan käyttää osoittamaan, että $\phi(n) = n - 1$.

Lause 4.4. *Olkoon $q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$ luvun $n - 1$ alkulukutekijöihinjako. Oletetaan, että jokaiselle luvulle i, kun $1 \leq i \leq k$, on olemassa luku a_i siten, että $a_i^{n-1} \equiv 1 \pmod{n}$ ja $a_i^{(n-1)/q_i} \not\equiv 1 \pmod{n}$. Tällöin n on alkuluku.*

Todistus. (Ks. [5, s. 188].) Näytetään, että jokainen $q_i^{e_i}$ jakaa luvun $\phi(n)$, ja että myös niiden tulo jakaa luvun $\phi(n)$.

Kiinnitetään indeksi i; jos a_i toteuttaa kongruenssin $a_i^{n-1} \equiv 1 \pmod{n}$, niin $\mathrm{ord}_n(a_i) \mid n-1$. Merkitään $n-1 = (\mathrm{ord}_n a_i)k$. Väitetään, että $q_i \nmid k$. Muuten

$$a_i^{(n-1)/q_i} \equiv a_i^{\mathrm{ord}_n a_i k/q_i} \equiv 1 \pmod{n}.$$

Tämä ei voi pitää paikkansa. Koska $\mathrm{syt}(q_i, k) = 1$, $q_i^{e_i}$ esiintyy luvun $n-1$ alkulukutekijöihinjaossa ja $n-1 = (\mathrm{ord}_n a_i)k$, on oltava $q_i^{e_i} \mid \mathrm{ord}_n a$. Siis $n-1 \mid \phi(n)$, mistä seuraa, että n on alkuluku. □

Esimerkki 4.6. (Ks. [5, s. 188].) Olkoon $n = 911$, $n-1 = 2 \cdot 5 \cdot 7 \cdot 13$. Voidaan laskea seuraavat kongruenssit:

$$\begin{aligned}
7^{n-1} &\equiv 1 \pmod{n} & 7^{(n-1)/2} &\equiv -1 \pmod{n} \\
3^{n-1} &\equiv 1 \pmod{n} & 3^{(n-1)/5} &\equiv 482 \pmod{n} \\
2^{n-1} &\equiv 1 \pmod{n} & 2^{(n-1)/7} &\equiv 568 \pmod{n} \\
2^{n-1} &\equiv 1 \pmod{n} & 2^{(n-1)/13} &\equiv 577 \pmod{n}.
\end{aligned}$$

Siis 911 on alkuluku lauseen 4.4 perusteella. Voidaan todistaa, että pienin primitiivinen juuri on 17. Edellä esitetty tapa on tehokkaampi kuin primitiivisen juuren etsiminen, koska siinä ei tarvitse hylätä jo laskettuja arvoja.

Seuraavat vaiheet kuuluvat luvun n jaottomuuden todistamiseen edellä mainitulla teorialla:

1. Annetaan luvun $n-1$ tekijöihinjako.
2. Jokaiselle luvun $n-1$ tekijälle q annetaan luku a, joska toteuttaa kongruenssin $a^{n-1} \equiv 1 \pmod{n}$ ja $a^{(n-1)/q} \not\equiv 1 \pmod{n}$.

Jos käytetään edellä esitettyjä alkulukutestejä, on välttämätöntä todistaa myös kaikkien luvun $n-1$ tekijöihinjaon alkioiden jaottomuus. Esimerkiksi esimerkin 4.5 täydellinen todistus sisältäisi luvun 1069 jaottomuuden todistuksen sekä muiden pienempien alkulukujen todistuksen, kunnes päästään lukuun 2. Tälläistä todistusta kutsutaan jaottomuussertifikaatiksi (eng. Primality certificate). Tämän tavan etu on sen helppo todistaminen. Voidaan kirjoittaa yksi ohjelma kehittämään sertifikaatti ja toinen todistamaan sen. Koska tämä sisältää ainoastaan potenssiinkorotusoperaatioita, on sen toteutus nopeaa.

4.4 Pocklingtonin alkulukutesti

Lause 4.5 (Pocklingtonin alkulukutesti)**.** *Olkoon n sellainen positiivinen kokonaisluku, että $n-1 = FR$, missä $\mathrm{syt}(F, R) = 1$ ja $F > R$. Kokonaisluku n on alkuluku, jos on olemassa kokonaisluku a siten, että $\mathrm{syt}(a^{(n-1)/q} - 1, n) = 1$, kun q on alkuluku siten, että $q \mid F$, ja $a^{n-1} \equiv 1 \pmod{n}$.*

Todistus. (Vrt. [8, s. 381].) Oletetaan, että p on luvun n alkulukutekijä. Koska oletuksen perusteella $a^{n-1} \equiv 1 \pmod{n}$ ja $p \mid n$, niin $a^{n-1} \equiv 1 \pmod{p}$. Tästä seuraa lauseen 2.13 perusteella, että $\mathrm{ord}_p a \mid n-1$. Siis on olemassa kokonaisluku t siten, että $n - 1 = t \cdot \mathrm{ord}_p a$.

Oletetaan seuraavaksi, että q on alkuluku, $q \mid F$ ja että q^e on luvun q potenssi, joka löytyy luvun F alkulukutekijähajotelmasta. Osoitetaan, että $q \nmid t$. Huomataan ensin, että jos olisikin niin, että $q \mid t$, niin silloin olisi olemassa luku l siten, että $t = ql$ ja saadaan kertaluvun määritelmän perusteella

$$a^{(n-1)/q} = a^{\mathrm{ord}_p a \cdot (t/q)} \equiv a^{\mathrm{ord}_p a \cdot l} \equiv 1 \pmod{p}.$$

Tästä seuraa, että $p \mid \mathrm{syt}(a^{(n-1)/q} - 1, n)$, koska $p \mid a^{(n-1)/q} - 1$ ja $p \mid n$. Tämä ei voi pitää paikkaansa, koska $\mathrm{syt}(a^{(n-1)/q} - 1, n) = 1$. Siis $q \nmid t$. Tästä seuraa, että $q^e \mid \mathrm{ord}_p a$. Koska jokaiselle alkuluvulle, joka jakaa luvun F, pätee, että kyseisen alkuluvun potenssi luvun F alkulukutekijähajotelmassa jakaa luvun $\mathrm{ord}_p a$, niin $F \mid \mathrm{ord}_p a$. Koska Fermat'n pienen lauseen ja kertaluvun määritelmän perusteella $\mathrm{ord}_p\, a \leq p-1$, niin $F \leq p - 1$, joten $F < p$.

Koska $F > R$ ja $n - 1 = FR$, niin $n - 1 < F^2$. Koska molemmat luvut $n - 1$ ja F^2 ovat kokonaislukuja, pätee, että $n \leq F^2$, ja koska sekä n että F ovat positiivisia, niin $F \geq \sqrt{n}$. Näin ollen $p > F \geq \sqrt{n}$. Koska $p \mid n$, niin $p = n$. Siis n on alkuluku. □

Seuraava esimerkki havainnollistaa Pocklingtonin alkulukutestin käyttöä, missä vain osaa luvun $n-1$ tekijähahmotelmasta on käytetty näyttämään, että n on alkuluku.

Esimerkki 4.7. Tässä esimerkissä näytetään, että 23801 on alkuluku, käyttämällä Pocklingtonin alkulukutestiä. Merkitään $n = 23801$, nyt voidaan käyttää luvun $n-1 = 23800 = FR$ osittaista tekijähajotelmaa, missä $F = 200 = 2^3 5^2$ ja $R = 119$, eli $F > R$. Valitaan $a = 3$ ja lasketaan Wolfam Alphan avulla, että

$$\begin{aligned} 3^{23800} &\equiv 1 \pmod{23801} \\ 3^{23800/2} &\equiv -1 \pmod{23801} \\ 3^{23800/5} &\equiv 19672 \pmod{23801}. \end{aligned}$$

Käyttämällä Wolfram Alphaa saadaan, että $\mathrm{syt}(3^{23800/2} - 1, 23801) = \mathrm{syt}(-2, 23801) = 1$ ja $\mathrm{syt}(3^{23800/5} - 1, 23801) = \mathrm{syt}(19671, 23801) = 1$. Tästä seuraa, että luku $n = 23801$ on alkuluku, vaikka ei ole käytetty luvun $n - 1 = 23800$ koko alkulukutekijähajotelmaa ($23800 = 2^3 \cdot 5^2 \cdot 7 \cdot 17$).

Pocklingtonin alkulukutestiä voidaan käyttää kehittämään uusi testi, joka on hyödyllinen, kun halutaan testata tietynmuotoisia alkulukuja.

Lause 4.6 (Prothin testi)**.** *Olkoon n positiivinen kokonaisluku siten, että $n = k2^m + 1$, missä k on pariton kokonaisluku ja m on kokonaisluku siten, että $k < 2^m$. Jos on olemassa kokonaisluku a siten, että*

$$a^{(n-1)/2} \equiv -1 \pmod{n}, \tag{4.3}$$

n on alkuluku.

Todistus. (Vrt. [8, s. 382].) Olkoon $s = 2^m$ ja $t = k$, joten $s > t$. Todistetaan, että $\text{syt}(a^{(n-1)/2} - 1, n) = 1$. Olkoon d sellainen luku, että $d \mid (a^{(n-1)/2} - 1)$ ja $d \mid n$. Silloin kongruenssin 4.3 perusteella $d \mid (a^{(n-1)/2} + 1)$. Tästä seuraa, että $d \mid (a^{(n-1)/2} + 1) - (a^{(n-1)/2} - 1) = 2$. Koska n on pariton, niin $d = 1$. Siis kaikki Pocklingtonin alkulukutestin hypoteesit täyttyvät, joten n on alkuluku. □

Esimerkki 4.8. Olkoon $n = 41$. Nythän $41 = 5 \cdot 2^3 + 1$. Eli luku 41 on Prothin testissä tarvittavaa muotoa. Jotta voidaan osoittaa, että n on alkuluku, täytyy kongruenssin $a^{(n-1)/2} \equiv -1 \pmod{n}$ pitää paikkaansa. Testaamalla ja laskemalla Wolfram Alphalla löydetään nopeasti vaadittu a;

$$a^{(n-1)/2} = 3^{20} \equiv 40 \equiv -1 \pmod{n}.$$

4.5 Millerin ja Rabinin alkulukutesti

Tässä aliluvussa esitellään Millerin ja Rabinin alkulukutestiä. Päinvastoin kuin esimerkiksi Fermat'n testi, Millerin ja Rabinin testi pystyy osoittamaan minkä tahansa yhdistetyn luvun jaollisuuden. Millerin ja Rabinin alkulukutesti pohjautuu Fermat'n pienen lauseen muunnelmaan.

Olkoon n pariton ja positiivinen kokonaisluku ja

$$s = \max\{r \in \mathbb{N} : 2^r \mid n - 1\},$$

eli 2^s on suurin luvun 2 potenssi, joka jakaa luvun $n - 1$. Merkitään

$$d = (n - 1)/2^s.$$

Nyt d on pariton.

Lause 4.7. *Olkoon G ryhmä. Jos $g \in G$ on äärellistä kertalukua e ja n on kokonaisluku, luvun g^n kertaluku on $e/\text{syt}(e, n)$.*

Todistus. (Ks. [1, s. 42].) □

Lause 4.8. *Jos n on alkuluku ja jos a on kokonaisluku siten, että n ja a ovat keskenään jaottomia lukuja, pätee*

$$a^d \equiv 1 \pmod{n}$$

tai on olemassa luku $r \in \{0, 1, ..., s - 1\}$ siten, että

$$a^{2^r d} \equiv -1 \pmod{n}.$$

Todistus. (Vrt. [1, s. 132].) Olkoon n alkuluku sekä a ja n keskenään jaottomia lukuja. Kertolaskuryhmän mod n kertaluku on $n - 1 = 2^s d$, koska n on alkuluku. Lauseen 4.7 mukaan jäännösluokan $a^d + n\mathbb{Z}$ kertaluku k on luvun 2 potenssi, koska

$$(n - 1)/\text{syt}(n - 1, d) = 2^s d/\text{syt}(2^s d, d) = 2^s d/d = 2^s.$$

Jos tämä kertaluku on $k = 1 = 2^0$,

$$(a^d)^1 \equiv a^d \equiv 1 \pmod{n}.$$

Jos $k > 1$, niin $k = 2^l$, kun $1 \leq l \leq s$. Lauseen 4.7 perusteella jäännösluokan $a^{2^{l-1}d} + n\mathbb{Z}$ kertaluku on 2, sillä

$$k/\mathrm{syt}(k, 2^{l-1}d) = 2^l/\mathrm{syt}(2^l, 2^{l-1}d) = 2^l/2^{l-1} = 2.$$

Kertolaskuryhmän $(\mathbb{Z}/n\mathbb{Z})^*$ ainoa kertalukua 2 oleva alkio on $-1 + n\mathbb{Z}$, koska kyseisen alkion tulee toteuttaa kongruenssi $b^2 \equiv 1 \pmod{n}$ ja ainoa alkio, millä kongruenssi pätee, on -1. Tästä seuraa

$$a^{2^r d} \equiv -1 \pmod{n}$$

kun $r = l - 1$. □

Jos n on alkuluku, niin ainakin toinen lauseen 4.8 väittämistä pätee. Joten, jos löydetään kokonaisluku a siten, että a ja n ovat keskenään jaottomia lukuja ja a toteuttaa toisen väittämistä jollain luvulla $r \in \{0, ..., s-1\}$, n on yhdistetty luku. Kyseistä lukua a kutsutaan luvun n jaollisuuden todistajaksi.

Esimerkki 4.9. (Vrt. [1, s. 133]). Olkoon $n = 561$. Koska n on Carmichaelin luku, Fermat'n testi ei pysty todistamaan sen jaollisuutta. Mutta $a = 2$ on todistaja luvun n jaollisuudelle, mikä näytetään seuraavaksi. Merkitään $s = 4$, $d = 35$ ja

$$\begin{aligned} 2^{35} &\equiv 263 \pmod{561} \\ 2^{2\cdot 35} &\equiv 166 \pmod{561} \\ 2^{4\cdot 35} &\equiv 67 \pmod{561} \\ 2^{8\cdot 35} &\equiv 1 \pmod{561}. \end{aligned}$$

Siis lauseen 4.8 perusteella nähdään, että 561 on yhdistetty luku.

Jotta Miller-Rabin alkulukutesti olisi tehokas, on tärkeää, että on olemassa mahdollisimman monta todistajaa luvun jaollisuudelle.

Esimerkki 4.10. (Ks. [1, s. 134-135].) Määritetään kaikki luvun $n = 15$ jaollisuuden todistajat. Nyt $n - 1 = 14 = 2 \cdot 7$, joten $s = 1$ ja $d = 7$. Kokonaisluku a, kun a ja n ovat keskenään jaottomia, on luvun n jaollisuuden todistaja, jos ja vain jos a^7 mod $15 \neq 1$ ja a^7 mod $15 \neq -1$. Seuraava taulukko sisältää jäännökset:

a	1	2	4	7	8	11	13	14
a^7 mod 15	1	8	4	13	2	11	7	14

Ainoa luku, joka ei ole todistaja, on 1.

Miller-Rabin alkulukutestiä parittomalle positiiviselle kokonaisluvulle käytetään niin, että valitaan sattumanvaraisesti luku $a \in \{2, 3, ..., n-1\}$. Jos $\mathrm{syt}(a, n) > 1$, n on yhdistetty luku. Muuten lasketaan $a^d, a^{2d}, ..., a^{2^{s-1}d}$. Jos löydetään luvun n jaollisuuden todistaja, on osoitettu, että n on yhdistetty luku.

4.6 Solovayn ja Strassenin alkulukutesti

Legendren symbolilla on olemassa yksi perusominaisuus, jota ei löydy Jacobin symbolilta: vastaavuus Eulerin kongruenssin $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$, jos $1 \leq a \leq p-1$, kanssa. Kyseisen kongruenssin luonnollinen vastaavuus parittomalle yhdistetylle luvulle mod n olisi

$$1 \leq a \leq n-1 \Rightarrow a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}, \tag{4.4}$$

mutta tämä ei kuitenkaan ole voimassa.

4.6.1 Euler-todistaja

Määritelmä 4.1. Jos n on pariton ja positiivinen kokonaisluku, silloin jos kokonaisluvulle $a \in \{1, ..., n-1\}$ pätee joko (i) $\text{syt}(a, n) > 1$ tai (ii) $\text{syt}(a, n) = 1$ ja $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$, niin lukua a kutsutaan luvun n Euler-todistajaksi.

Jos n on pariton alkuluku, kumpikaan ehdoista (i) tai (ii) eivät päde millään luvulla $a \in \{1, ..., n-1\}$, joten tällöin luvulla n ei ole yhtään Euler todistajaa. Siis luvun n yhdenkin Euler todistajan olemassaolo todistaa luvun n jaollisuuden, mutta olemassaolo ei kuitenkaan kerro, miten miten n voidaan jakaa tekijöihin.

Ehto $\text{syt}(a, n) > 1$ on yhtäpitävä ehdon $\left(\frac{a}{n}\right) = 0$ kanssa, joten ei tarvitse testata ehtoja $\text{syt}(a, n) > 1$ ja $\text{syt}(a, n) = 1$ erikseen, jos yritetään selvittää, onko luku Euler todistaja. Jos lasketaan kongruenssi $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, se paljastaa onko $\text{syt}(a, n) > 1$, kun kongruenssin oikea puoli on 0.

On hieman helpompaa selvittää, milloin luku a ei ole luvun n Euler todistaja kuin milloin se on. Se, että a ei ole luvun n Euler todistaja, tarkoittaa, että ehdot

$$\text{syt}(a, n) = 1 \text{ ja } a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}, \tag{4.5}$$

toteutuvat, ja ehto $\text{syt}(a, n) = 1$ on yhtäpitävä ehdon $\left(\frac{a}{n}\right) = \pm 1$ kanssa.

Esimerkki 4.11. (Ks. [3, s. 1-2].) Olkoon $n = 1387$. Koska

$$2^{(n-1)/2} = 2^{693} \equiv 512 \not\equiv \pm 1 \pmod{1387},$$

luku 2 on luvun n Euler todistaja. Luvulla n on 1224 Euler todistajaa, mikä on noin 88,2% nollasta eroavista luvuista mod n.

Esimerkki 4.12. (Ks. [3, s. 2].) Olkoon $n = 49141$. Alla olevasta taulukosta nähdään, että luku 5 on luvun 49141 Euler todistaja.

a	$a^{(n-1)/2} \pmod{n}$	$\left(\frac{a}{n}\right)$
2	-1	-1
3	1	1
4	1	1
5	8163	1

Luvulla n on 36972 Euler todistajaa, mikä on noin 75,2% nollasta eroavista luvuista mod n.

Esimerkki 4.13. (Ks. [3, s. 1].) Olkoon $n = 75361$. Alla olevasta taulukosta nähdään, että luku 7 on Euler todistaja.

a	$a^{(n-1)/2} \pmod n$	$\left(\frac{a}{n}\right)$
2	1	1
3	1	1
4	1	1
5	1	1
6	1	1
7	1	-1

Toisin kuin kahdessa aiemmassa esimerkissä ensimmäisellä Euler todistajalla 7 pätee $a^{(n-1)/2} \equiv \pm 1 \pmod n$, mutta merkki ei ole $\left(\frac{a}{n}\right)$. Kongruenssi (4.4) on tarkempi kuin $a^{(n-1)/2} \equiv \pm 1 \pmod n$. Luvulla n on 46560 Euler todistajaa, mikä on noin 61,7% nollasta eroavista luvuista mod n.

4.6.2 Solovayn ja Strassenin lause

Jos yritetään selvittää, onko n alkuluku, etsimällä Fermat'n testillä vastaesimerkkiä kongruenssille $a^{n-1} \equiv 1 \pmod n$ luvuista $1, .., n-1$, tiedetään, että vastaesimerkkien määrä suhteessa Fermat'n todistajiin on suurempi kuin 50%, jos n on yhdistetty ja n ei ole Carmichaelin luku. Jos n taas on Carmichaelin luku, ainoat vastaesimerkit kongruenssille $a^{n-1} \equiv 1 \pmod n$ ovat sellaiset luvut a, joille pätee $\text{syt}(a, n) > 1$, ja tällöin kyseisten lukujen a määrä voi olla hyvin pieni. Seuraavat Solovayn ja Strassenin teoriat esittävät, että tällaista ongelmaa ei ole Eulerin kongruenssille, koska sitä käsitellessä ei ole mitään Carmichaelin lukujen kaltaisia lukuja.

Lause 4.9. *[Solovayn ja Strassenin lause] Olkoon n pariton, yhdistetty sekä positiivinen kokonaisluku. Nyt on olemassa kokonaisluku a siten, että* $\text{syt}(a, n) = 1$ *ja* $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod n$.

Todistus. (Ks. [3, s. 2-3].) Tehdään todistus kahdessa osassa. Ensimmäisessä osassa oletetaan, että luvulla n ei ole yhtään tekijää, joka olisi korotettu potenssiin. Toisessa osassa oletetaan, että tälläinen löytyy.

Oletetaan siis, että n on yhdistetty luku, jolla ei ole yhtään tekijää, joka olisi korotettu potenssiin > 1. Nyt $n = p_1 p_2 \cdots p_r$, kun $r \geq 2$ ja kaikki p_i:t ovat erisuuria parittomia alkulukuja. Puolet nollasta eroavista luvuista mod p_1 eivät ole neliöitä, joten on olemassa $b \in \mathbb{Z}$ siten, että $\left(\frac{b}{p_1}\right) = -1$. Kiinalaisen jäännöslauseen perusteella on olemassa $a \in \mathbb{Z}$, joka toteuttaa seuraavat kongruenssit:

$$a \equiv b \pmod{p_1}, \quad a \equiv 1 \pmod{p_2 \cdots p_r}.$$

Nyt siis luvut a ja p_1 ovat keskenään jaottomia ja sama pätee luvuille a ja $p_2 \cdots p_r$, joten $\text{syt}(a, n) = 1$. Myös $\left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1$ ja $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right) = 1$, kun $i > 1$, joten

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right) = \left(\frac{a}{p_1}\right) = -1.$$

Oletetaan, että $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, joten $a^{(n-1)/2} \equiv -1 \pmod{n}$. Koska p_2 jakaa luvun n, kongruenssista $a^{(n-1)/2} \equiv -1 \pmod{n}$ seuraa, että $a^{(n-1)/2} \equiv -1 \pmod{p_2}$, mistä saadaan

$$1 \equiv -1 \pmod{p_2},$$

koska $a \equiv 1 \pmod{p_2}$. Tämä ei voi pitää paikkaansa, koska modulus p_2 on suurempi kuin 2.

Oletetaan nyt, että luvulla n on toistuva alkulukutekijä. Merkitään sitä kirjaimella p. Silloin $n = p^k m$, missä $k \geq 2$ ja $\text{syt}(p, m) = 1$. Kiinalaisen jäännöslauseen mukaan on olemassa $a \in \mathbb{Z}$, joka toteuttaa kongruenssit

$$a \equiv 1 + p \pmod{p^2}, \quad a \equiv 1 \pmod{m}.$$

Nyt $a = k \cdot p^2 + 1 + p$ jollakin luvulla $k \in Z$. Tästä seuraa, että luku a ei ole jaollinen luvulla p. Koska $a - 1 \equiv 0 \pmod{m}$, $\text{syt}(a, m) = 1$, joten $\text{syt}(a, n) = 1$. Jos $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, korottaminen toiseen potenssiin saa aikaan seuraavan kongruenssin $a^{n-1} \equiv 1 \pmod{n}$, ja tavoitteena on osoittaa, että kyseinen kongruenssi ei voi pitää paikkaansa. Vähennetään kongruenssi modulo p^2:ksi, jotta saadaan kongruenssi $a^{n-1} \equiv 1 \pmod{p^2}$. Koska $a \equiv 1 + p \pmod{p^2}$, saadaan $(1 + p)^{n-1} \equiv 1 \pmod{p^2}$. Käyttämällä binomikaavaa saadaan $(1 + p)^{n-1} \equiv 1 + (n - 1)p \pmod{p^2}$, joten $1 + (n - 1)p \equiv 1 \pmod{p^2}$. Vähentämällä luku 1 molemmilta puolilta saadaan $(n-1)p \equiv 0 \pmod{p^2}$, joten $n - 1 \equiv 0 \pmod{p}$. Nyt siis $n \equiv 1 \pmod{p}$, mutta luku p on luvun n toistuva alkulukutekijä, joten jakamalla luku n luvulla p ei voida saada jäännökseksi lukua 1. □

Lause 4.10. *Olkoon $n > 1$ pariton kokonaisluku.*

1. *Jos n on alkuluku, niin* $|\{1 \leq a \leq n - 1 | a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}\}| = n - 1.$
2. *Jos n on yhdistetty luku, niin* $|\{1 \leq a \leq n - 1 |\, \text{syt}(a, n) = 1$ *ja* $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}\}| < \frac{n-1}{2}$.

Todistus. (Ks. [3, s. 3-4].)Kohdan 1. todistus seuraa suoraan Eulerin kriteeristä. Jotta voidaan todistaa kohta 2., muistetaan ensin, että $\left(\frac{a}{n}\right) = \pm 1$, jos $\text{syt}(a, n) = 1$, ja $\left(\frac{a}{n}\right) = 0$, jos $\text{syt}(a, n) > 1$. Merkitään

$$A = \{1 \leq a \leq n - 1 \mid \text{syt}(a, n) = 1 \text{ ja } a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}\},$$
$$B = \{1 \leq a \leq n - 1 \mid \text{syt}(a, n) = 1 \text{ ja } a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}\},$$
$$C = \{1 \leq a \leq n - 1 \mid \text{syt}(a, n) > 1\}.$$

Joukot A, B ja C ovat erillisiä ja käsittävät kaikki kokonaisluvut $1, ..., n-1$. Joukko A ei ole tyhjä, koska $1 \in A$. Joukko C ei ole tyhjä, koska n on yhdistetty luku. Lauseen 4.9 mukaan myöskään joukko B ei ole tyhjä. Tavoitteena on osoittaa, että $|A| < (n-1)/2$.

Valitaan joukosta B luku b_0. Osoitetaan, että joukko $Ab_0 = \{ab_0 \pmod n \mid a \in A\}$ on joukon B osajoukko, missä "$ab_0 \pmod n$"tarkoittaa jäännöstä, kun ab_0 jaetaan luvulla n. Jokaiselle $a \in A$ pätee, että tulo ab_0 ja n ovat keskenään jaottomia ja

$$(ab_0)^{(n-1)/2} \equiv a^{(n-1)/2} b_0^{(n-1)/2} \equiv \left(\frac{a}{n}\right) b_0^{(n-1)/2} \pmod n.$$

Joko $ab_0 \bmod n$ kuuluu joukkoon A tai joukkoon B. Jos $(ab_0 \bmod n) \in A$, niin $(ab_0)^{(n-1)/2} \equiv \left(\frac{ab_0}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b_0}{n}\right) \pmod n$, joten $\left(\frac{a}{n}\right)\left(\frac{b_0}{n}\right) \equiv \left(\frac{a}{n}\right) b_0^{(n-1)/2} \pmod n$. Koska $\mathrm{syt}(a, n) = 1$, saadaan $\left(\frac{a}{n}\right) = \pm 1$, joten kongruenssin molemmilta puolita voidaan jakaa $\left(\frac{a}{n}\right)$, jolloin saadaan $\left(\frac{b_0}{n}\right) \equiv b_0^{(n-1)/2} \pmod n$, mikä on ristiriita, koska b_0 kuuluu joukkoon B. Siis $ab_0 \bmod n \in B$ kaikilla $a \in A$, joten $Ab_0 \subset B$.

Oletetaan, että luvut a ja a' kuuluvat joukkoon A. Jos $ab_0 \equiv a'b_0 \pmod n$, niin jaetaan b_0 molemmilta puolilta. Tämä voidaan tehdä, koska $\mathrm{syt}(b_0, n) = 1$. Näin saadaan $a \equiv a' \pmod n$, joten $a = a'$, koska joukon A alkiot kuuluvat joukkoon $\{1, 2, ..., n-1\}$.. Siis joukon Ab_0 alkioiden lukumäärä on $|A|$, joten koska $Ab_0 \subset B$, saadaan $|A| = |Ab_0| \leq |B|$. Siis

$$n - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|,$$

joten $n - 1 > 2|A|$. Nyt siis $|A| < (n-1)/2$. □

Lause 4.11. *Olkoon $n > 1$ pariton kokonaisluku. Luvun n Euler todistajien määrä kokonaisluvuista $1, ..., n-1$ on 0%, jos n on alkuluku, ja yli 50%, jos n on yhdistetty luku.*

Todistus. (Ks. [3, s. 4].) Parittomalla alkuluvulla ei ole ollenkaan Euler todistajia Eulerin kongruenssin mukaan. Lauseen 4.10 mukaan, jos n on yhdistetty luku, niiden lukujen, jotka eivät ole Euler todistajia, määrä luvuista $1, ..., n-1$ on pienempi kuin 50%, joten Euler todistajien määrä luvuista $1, ..., n-1$ on suurempi kuin 50%. □

Kahtiajako luvun n Euler todistajien lukumäärässä, kun n on alkuluku tai yhdistetty luku, on todella merkittävä. Tästä seuraa Solovayn ja Strassenin alkulukutesti, missä testataan, onko $n > 1$ alkuluku. Testi perustuu korkeisiin todennäköisyyksiin löytää luvun n Euler todistaja, kun n on yhdistetty, verrattuna siihen, että luvun n Euler todistajia ei ole olemassa, jos n on alkuluku.

Testi menee karkeasti näin:

1. Valitse kokonaisluku $t \geq 1$, joka on testin kokeilujen lukumäärä.
2. Valitse satunnainen kokonaisluku $a \in \{1, ..., n-1\}$.
3. Jos (4.5) ei päde luvulle a, lopeta testi ja totea, että n on yhdistetty luku.

4. Jos (4.5) pätee luvulle a, mene takaisin kohtaan 2.

5. Jos testin kokeilujen lukumäärä tulee täyteen ennen kuin testi loppuu, totea, että n on alkuluku vähintään todennäköisyydellä $1 - 1/2^t$.

Todennäköisyys $1 - 1/2^t$ testin viimeisessä kohdassa saadaan siitä, että yli puolet luvuista $1, ..., n - 1$ ovat luvun n Euler todistajia, jos n on yhdistetty luku. Todennäköisyys sille, että t kokeilun jälkeen ei löydy Euler todistajaa luvulle n, kun n on yhdistetty luku, on yhtä todennäköistä kuin kolikon heittäminen ilmaan t kertaa ja joka kerta sama puoli on ylöspäin. Itse asiassa se on vähemmän todennäköistä kuin kolikon heittely, koska Euler todistajien määrä on suurempi kuin 50%. Siis todennäköisyys, että n on alkuluku, jos luvulle n ei löydy yhtään Euler todistajaa t kokeilun jälkeen on suurempi kuin $1 - 1/2^t$.

Huomautus 4.1. Yllä esitetty todennäköisyyspäättely ei ole täysin pätevä, mutta virhe ei käytännössä ole merkittävä, joten sitä ei käsitellä tässä. Lisätietoja löytyy kuitenkin haluttaessa lähteestä [3].

Solovayn ja Strassenin testissä luku $a \in \{1, ..., n-1\}$ valitaan sattumanvaraisesti, ei järjestelmällisesti. Osin niin tehdään, jotta vältytään tarpeettomalta tiedolta. Esimerkiksi esimerkissä 4.13 kohdat $a = 4$ ja $a = 6$ ovat täysin riippuvaisia kohdista $a = 2$ ja $a = 3$, koska jos kongruenssi $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ ja ehto $\text{syt}(a, n) = 1$ pätee kahdelle luvun a arvolle, pätee se myös niiden tulolle.

Esimerkki 4.14. (Ks. [3, s. 4-5].) Olkoon $n = 56052361$. Alla olevassa taulukossa listataan sattumanvaraisesti valittuja lukuja a luvuista $1, ..., n - 1$ ja löydetään eroavaisuus 3 kokeilun jälkeen, mikä todistaa, että n on yhdistetty luku. Kuitenkaan tästä ei saada luvun n tekijöihin jakoa. Se, että tietää luvun olevan yhdistetty, ei tarkoita, että tietäisi tekijöihinjaon.

a	$a^{(n-1)/2} \pmod{n}$	$\left(\frac{a}{n}\right)$
40715161	1	1
18267097	1	1
55146139	1	-1

Brute-force-laskennalla luvun n Euler todistajien lukumäärä on 27783000, joka on juuri yli puolet kaikista luvuista $1, .., n - 1$: $\frac{27783000}{56052360} \approx 0,5043$. Alaraja sille, että vähintään puolet luvuista ovat Euler todistajia, näyttää olevan suhteellisen tiukka.

50 prosentin alaraja parittomien yhdistettyjen lukujen Euler todistajien määrälle on todennäköisesti tiukka: jos $6k + 1$,$12k + 1$ ja $18k + 1$ ovat kaikki alkulukuja, joten Euler todistajien määrä tulolle $(6k + 1)(12k + 1)(18k + 1)$ on 50%, kun $k \to \infty$. (On oletettu, että $6k + 1$,$12k + 1$ ja $18k + 1$ ovat jaottomia äärettömän usein.)

Esimerkki 4.15. (Ks. [3, s. 5].) Olkoon $n = 7427466391$. Alla olevassa taulussa esitetään 10 kokeilun tulos, mikä on se, että luvulle ei löydy yhtään Eulerin todistajaa.

a	$a^{(n-1)/2} \pmod{n}$	$\left(\frac{a}{n}\right)$
3402235571	1	1
2277339183	1	1
3511612661	1	1
1892495979	-1	-1
735536755	1	1
966099371	-1	-1
3288169902	1	1
3037671250	-1	-1
270193898	1	1
7427466390	-1	-1

Jos luku n olisi yhdistetty luku, sen todennäköisyys olisi noin $1/2^{10} \approx 0,00097$, joten on luonnollista uskoa, että n on alkuluku, mutta taulukko ei kuitenkaan todista sitä. (Luku n on todellakin alkuluku, minkä tietokone pystyy tarkistamaan helposti kymmennumeroiselle luvulle.)

Lähteet

[1] Buchmann, J. A. *Introduction to Cryptography*, Springer, Heidelberg, 1999.

[2] Conrad, K. *Carmichael Numbers and Korselt's Criterion*, Viitattu: 19.5.2017, URL: http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/carmichaelkorselt.pdf

[3] Conrad, K. *The Solovay-Strassen Test*, Viitattu: 26.3.2017, URL: http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/solovaystrassen.pdf

[4] Koblitz, N. *A Course in Number Theory and Cryptography*, Springer, New York, 1998.

[5] Kumanduri, R., Romero, C. *Number Theory with Computer Applications*, Prentice Hall, New Jersey, 1998.

[6] Long, C. T. *Elementary Introduction to Number Theory*, 3rd ed., Waveland Press, Inc., Illinois, 1995.

[7] Molin, R. A. *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, 1998.

[8] Rosen, K. H. *Elementary Number Theory and Its Applications*, 6th ed., Pearson Education Limited, Essex, 2014.

[9] Wagstaff, S. S. Jn. *Cryptanalysis of Number Theoretic Ciphers*, CRC Press, Boca Raton, 2003.